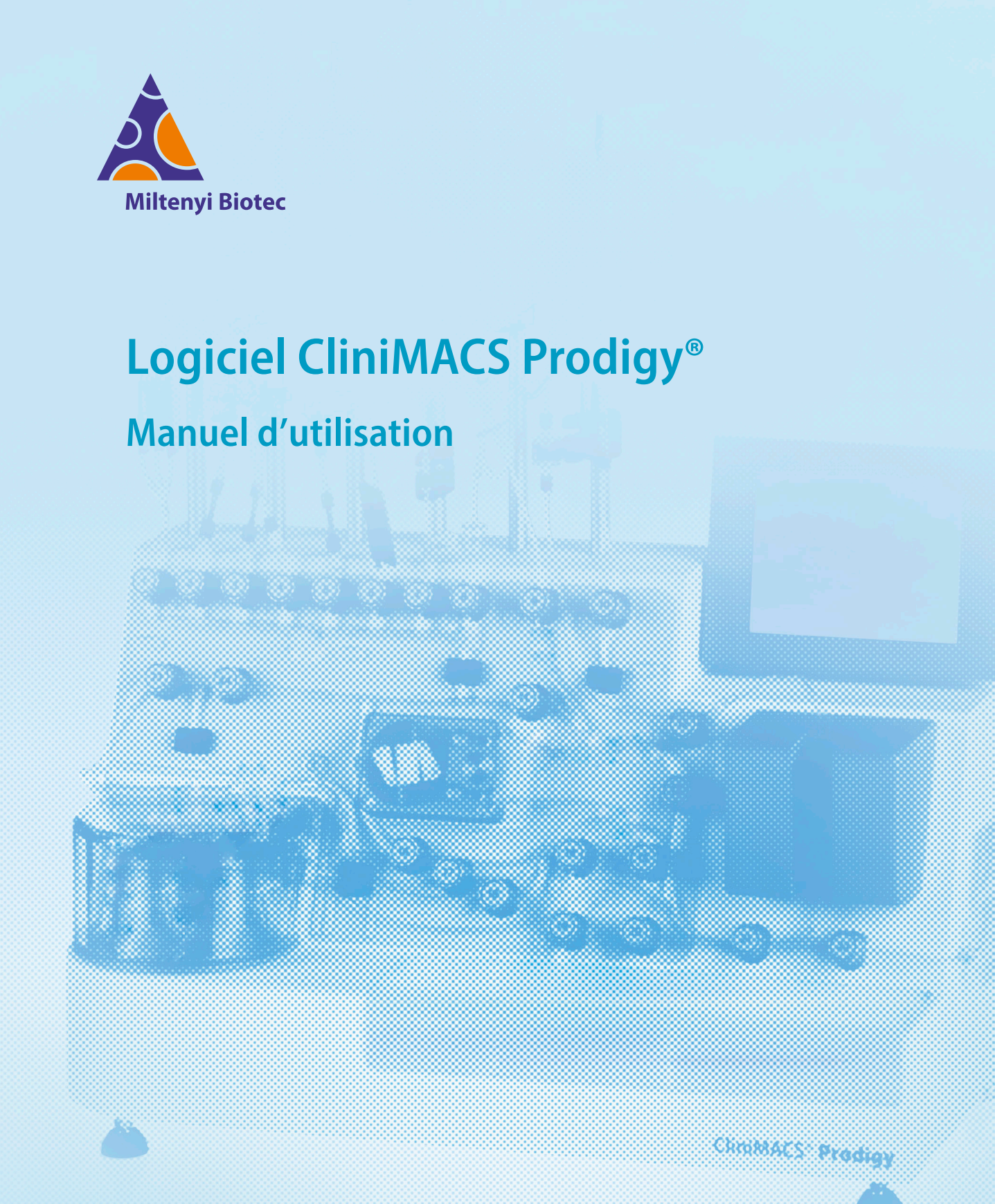
Miltenyi Biotec

Logiciel CliniMACS Prodigy®

Manuel d’utilisation



Les éléments du système CliniMACS incluant réactifs, jeux de tubulures, instruments et tampon PBS/EDTA, sont conçus, fabriqués et testés selon un système de qualité certifié ISO 13485. Dans les pays de l'UE, les éléments du système CliniMACS sont disponibles en tant que dispositifs médicaux marqués CE, pour l'usage respectivement prévu, sauf indication contraire. Aux États-Unis, le système CliniMACS CD34 Reagent incluant le CliniMACS Plus Instrument, le CliniMACS CD34 Reagent, le CliniMACS Tubing Set TS et le CliniMACS Tubing Set LS ainsi que le CliniMACS PBS/EDTA Buffer, est approuvé par la FDA en tant que dispositif à usage humanitaire (HUD) et autorisé par la loi fédérale des États-Unis pour le traitement de patients atteints de leucémie aiguë myéloïde (LAM) en première rémission complète. L'efficacité de ce dispositif n'a pas été démontrée pour cette indication. Tous les autres produits de la gamme CliniMACS sont uniquement disponibles pour une utilisation dans le cadre d'une demande approuvée de nouveau médicament expérimental (IND), d'une exemption de dispositif expérimental (IDE) ou d'une approbation de la FDA. En Australie, les composants suivants du système CliniMACS Prodigy sont compris dans l'Australian Register of Therapeutic Goods (ARTG) et sont donc approuvés pour livraison : CliniMACS Prodigy, CliniMACS CD34 Reagent, jeux de tubulures CliniMACS Prodigy et CliniMACS PBS/EDTA Buffer. Seuls ces produits compris dans l'ARTG peuvent être utilisés en Australie. Les CliniMACS MicroBeads sont uniquement destinés à des fins de recherche et non à l'usage thérapeutique humain ou diagnostique.

Sauf mention spécifique contraire, les produits et services de Miltenyi Biotec sont destinés uniquement à la recherche et non à des fins thérapeutiques ou diagnostiques.

Copyright © 2026 Miltenyi Biotec et/ou ses filiales. Tous droits réservés.

Aucune partie de cette publication ne peut être reproduite, sauvegardée sur un système de recherche, transmise, publiée, ni diffusée sous quelque forme que ce soit ou par quelconque moyen électronique, mécanique, par photocopie, microfilm, enregistrement ou autre, sans l'autorisation écrite préalable de Miltenyi Biotec. Toutefois, nonobstant ce qui précède, les propriétaires du système CliniMACS Prodigy peuvent faire des copies aux seules fins de la formation du personnel dans l'utilisation ou l'entretien de l'unité au sein de leur entreprise ou organisation.

CliniMACS, CentriCult et le logo Miltenyi Biotec sont des marques ou marques déposées de Miltenyi Biotec B.V. & Co. KG et/ou de ses filiales dans différents pays du monde. Toutes les autres marques commerciales mentionnées dans cette documentation ou dans tout autre document d'accompagnement sont la propriété de leurs propriétaires respectifs et ne sont utilisés qu'à des fins d'identification.

Logiciel CliniMACS Prodigy®

Manuel d'utilisation

Logiciel version 2.2

Édition : 2026-03

210-005-266/01

MD CE 0123

Miltenyi Biotec B.V. & Co. KG
Friedrich-Ebert-Straße 68
51429 Bergisch Gladbach
Allemagne

Miltenyi Biotec Technical Support
+49 2204 8306-3803
technicalsupport@miltenyi.com

www.miltenyibiotec.com

Informations essentielles

Ce manuel d'utilisation contient des instructions, des avertissements, des précautions d'emploi, des remarques et d'autres informations importantes pour l'utilisation du logiciel CliniMACS Prodigy. Pour des informations détaillées concernant l'instrument, telles que l'écran tactile et la configuration générale, se reporter au manuel d'utilisation de l'instrument CliniMACS Prodigy.

⚠ AVERTISSEMENT

L'utilisation du système CliniMACS Prodigy doit être effectuée uniquement par des opérateurs formés. Avant de mettre en service le système, l'opérateur doit avoir lu attentivement et compris les consignes de sécurité, avertissements, précautions d'emploi et instructions pour l'utilisation correcte du CliniMACS Prodigy, fournis dans les notices d'utilisation des éléments du système CliniMACS Prodigy et dans toutes les recommandations liées à la sécurité publiées par Miltenyi Biotec. Ces notices d'utilisation comprennent, mais sans s'y limiter, les consignes de sécurité figurant dans le manuel d'utilisation de l'instrument CliniMACS Prodigy, chapitre 3 « Informations importantes sur la sécurité ». Accorder une attention particulière à tous les avertissements affichés sur l'instrument ou fournis avec les consommables et les accessoires ainsi qu'aux remarques et informations importantes figurant dans ce manuel d'utilisation. Suivre en permanence toutes les instructions et procédures pendant l'utilisation de l'instrument, en veillant à respecter toutes les consignes de sécurité, les avertissements, les précautions d'emploi et les instructions. Le non-respect des consignes de sécurité et des informations importantes, avertissements, précautions d'emploi, remarques complémentaires et instructions figurant dans les notices d'utilisation pourrait se traduire par un dysfonctionnement de l'instrument, des dommages matériels, des blessures corporelles et/ou la mort. La sécurité de l'équipement peut être compromise si l'instrument n'est pas utilisé conformément aux instructions du fabricant. Conserver les notices d'utilisation pour pouvoir les consulter ultérieurement. Elles doivent être accessibles et rapidement consultables, comme tous les autres documents sur la sécurité et le fonctionnement, pour tout le personnel chargé de l'installation, de l'utilisation et de l'entretien, et ce, pendant toute la durée de vie de l'instrument.

Table des matières

1	**Introduction**	**9**
1.1	Informations générales	9
1.2	Informations réglementaires	10
1.3	Lois sur la protection des données	10
1.4	À propos de ce manuel	11
1.5	Documents associés	11
2	**Glossaire**	**13**
2.1	Niveau de danger	13
2.2	Conventions de présentation	14
2.3	Glossaire des symboles et des termes	14
2.3.1	Termes spécifiques au logiciel	14
3	**Informations importantes sur la sécurité**	**17**
3.1	Consignes de sécurité pour le CliniMACS Prodigy	17
3.2	Consignes de sécurité pour le logiciel	17
4	**Cybersécurité**	**19**
4.1	Concept de sécurité de défense en profondeur	19
4.1.1	Couche de protection physique	20
4.1.2	Couche d'environnement réseau	21
4.1.3	Couche de logiciel de l'instrument	24
4.1.4	Couche de l'utilisateur	25
4.1.5	Couche d'audit	25
4.1.6	Couche de gestion des mises à jour	26
4.1.7	Couche de gestion de la vulnérabilité	26
4.1.8	Couche de sauvegarde et de récupération	26
4.1.9	Résumé de la configuration sécurisée	27

5	**Concept logiciel**	**29**
5.1	Concept de base	29
5.2	Interface graphique utilisateur	30
5.2.1	Barre de menu et zone de contenu	31
5.2.2	Ligne d'état	32
5.2.3	Barre d'outils	32
5.2.4	Champs de saisie	34
5.2.5	Fenêtres contextuelles	35
6	**Fonctionnement de base**	**37**
6.1	Mise sous tension de l'instrument	37
6.2	Connexion	38
6.3	Logout (Déconnexion)	39
6.4	Arrêt	39
6.5	Arrêt d'urgence	39
6.6	Sélectionner un processus d'application	40
6.7	Exécuter un processus d'application	41
6.8	Mettre un processus d'application en pause	42
6.9	État de l'instrument et du processus d'application	43
6.10	Acquisition d'images	44
6.10.1	Layer Detection Camera	45
6.10.2	Caméra microscope	46
7	**Accès aux données**	**47**
7.1	Récupération des journaux d'application	47
7.1.1	Affichage et exportation des fichiers journaux vers une clé USB	47
7.1.2	Récupération via FTP	49
7.1.3	Récupération des fichiers via le partage des fichiers	50
7.2	Récupération de piste d'audit	51
7.2.1	Affichage de la piste d'audit	52
7.2.2	Exportation de la piste d'audit	53
7.2.3	Suppression de la piste d'audit	55

8 Outils et paramètres utilisateur 57

8.1 Accès aux outils et paramètres utilisateur 57
8.2 Tools (Outils) 58
8.2.1 Info tool (Outil Info) 58
8.2.2 Backup Filed Data (Sauvegarde des données archivées) 59
8.2.3 Chamber In (Insertion de la chambre) 63
8.2.4 Chamber Out (Retrait de la chambre) 63
8.2.5 Shutdown (Arrêt) 64
8.2.6 Recovery (Récupération) 64
8.2.7 Gas Mix tool (Outil pour mélange des gaz) 64
8.2.8 Instrument Check (Contrôle de l'instrument) 65
8.2.9 Column Load (Chargement des colonnes) 65
8.2.10 Custom Files (Fichiers personnalisés) 65
8.2.11 Sealer (Soudeuse) 65
8.3 User settings (Paramètres utilisateur) 65
8.3.1 Set time (Réglage date et heure) 65
8.3.2 Network Settings (Paramètres réseau) 65
8.3.3 Customer settings (Paramètres client) 66
8.3.4 Module settings (Paramètres du module) 66
8.3.5 Settings Exchange (Partage de paramètres) 67
8.3.6 SetVolume (Réglage du volume) 71
8.3.7 N_2 Settings (Paramètres N_2) 71

9 Intégration au réseau 73

9.1 Connexion à un réseau local 74
9.2 Connexion à un serveur de LDAP 76
9.3 Connexion à une unité du réseau 80
9.4 Configuration du transfert des fichiers via FTP 83
9.4.1 Paramétrage de l'instrument 84
9.4.2 Connexion au client FTP 85
9.5 Connexion à un serveur de courriel 86
9.6 Activation de la synchronisation de l'heure avec le réseau 91

10 Gestion des utilisateurs 93

10.1 Informations générales 93
10.2 Gestion des rôles et des comptes 96
10.2.1 Accès à la gestion des utilisateurs 96
10.2.2 Création d'un nouveau rôle 97
10.2.3 Modification des droits des rôles 98
10.2.4 Ajout d'un utilisateur local 98
10.2.5 Ajout d'utilisateurs LDAP 102
10.2.6 Ajout de groupes LDAP 104
10.2.7 Modification des rôles attribués à un utilisateur ou à un groupe LDAP 105
10.2.8 Désactivation d'utilisateurs locaux 105
10.2.9 Suppression d'utilisateurs LDAP 107
10.3 Configuration de la politique en matière de mots de passe 108
10.4 Importation et exportation des paramètres de gestion des utilisateurs 109
10.4.1 Exportation des paramètres de gestion des utilisateurs 110
10.4.2 Importation des paramètres UMS 112

11 Dépannage 115

12 Mentions légales 117

12.1 Limites de garantie 117
12.2 Marques commerciales 118

ANNEXE

1 Introduction

1.1 Informations générales

Le logiciel du CliniMACS Prodigy comprend une plateforme de base appelée « logiciel noyau » et divers logiciels d'application.

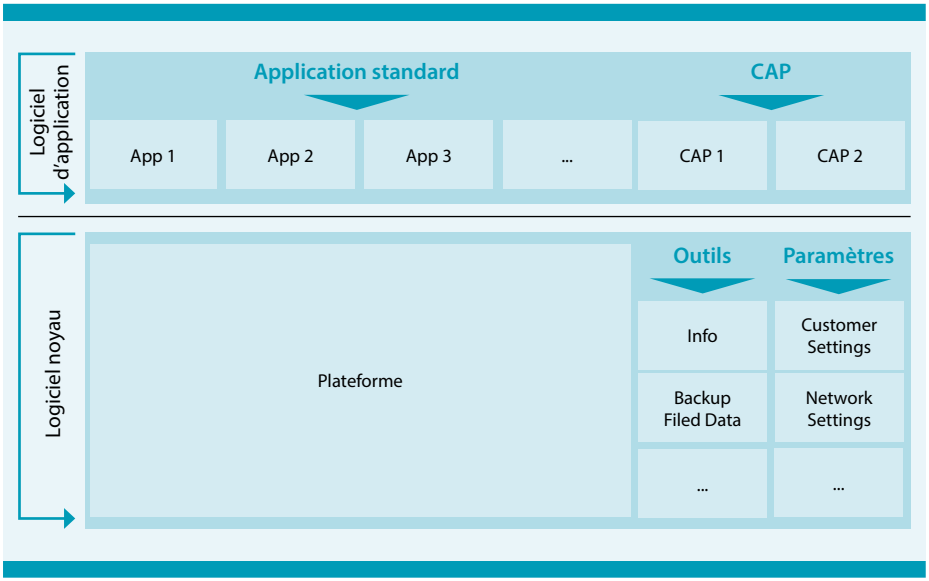


Figure 1.1: Aperçu du logiciel de l'instrument

Le logiciel noyau contrôle l'instrument et l'exécution des processus d'application et fournit les services essentiels décrits dans les différents chapitres et sections correspondants.

Le logiciel noyau est également appelé logiciel dans ce manuel d'utilisation.

Le logiciel d'application est exécuté par le logiciel noyau et fournit les processus d'application et les interfaces utilisateur pour le fonctionnement du CliniMACS Prodigy en fonction de son utilisation prévue :

- en tant qu'élément du système CliniMACS Prodigy pour la séparation cellulaire destiné à la séparation de cellules humaines
- en tant qu'élément du système de production CliniMACS Prodigy pour thérapies cellulaires et géniques, destiné aux étapes de manipulation génétique et/ou d'autre manipulation substantielle (telle que la prolifération, la différenciation) de cellules humaines.

Le logiciel noyau et chaque application sont des éléments indépendants, ce qui permet de mettre à jour séparément une nouvelle application sans modifier le logiciel noyau.

1.2 Informations réglementaires

Le logiciel a été développé conformément à la norme CEI/EN 62304. En outre, le logiciel noyau du CliniMACS Prodigy a été développé pour assurer la conformité aux normes GAMP 5, EudraLex Volume 4 Annexe 11 (EU GMP Annexe 11) et 21 CFR Part 11.

Les exigences en matière de cybersécurité de la norme CEI 81001-5-1 sont respectées, y compris les tests de pénétration effectués par une société tierce.

L'aperçu complet des informations réglementaires, y compris la destination, figure dans le manuel d'utilisation de l'instrument CliniMACS Prodigy.

1.3 Lois sur la protection des données

Lors du traitement de données personnelles avec le système CliniMACS Prodigy, la discrétion de l'utilisateur est fortement recommandée. Il est de la responsabilité de l'utilisateur de s'assurer de la conformité vis-à-vis des lois et règlementations en vigueur en matière de protection des données.

Conformément aux principes de protection des données dès la conception et par défaut, Miltenyi a mis en place des mesures de sécurité, en particulier le concept de défense en profondeur (voir paragraphe 4.1 « Concept de sécurité de défense en profondeur »).

1.4 À propos de ce manuel

Ce manuel d'utilisation fournit les informations nécessaires pour la configuration et le fonctionnement en toute sécurité du logiciel noyau. Ce manuel d'utilisation couvre uniquement le logiciel noyau 2.2.

1.5 Documents associés

Le manuel d'utilisation de l'instrument CliniMACS Prodigy décrit le matériel et le système de l'instrument CliniMACS Prodigy. Celui-ci est fourni avec le présent manuel.

Le manuel d'utilisation de l'instrument comprend :

- Avertissements, précautions d'emploi, remarques
- Informations règlementaires
- Caractéristiques techniques
- D'autres informations importantes

Si le CliniMACS Prodigy est utilisé avec le MACS® TubeSealer, le CliniMACS Electroporator, la CliniMACS Formulation Unit ou le CliniMACS Workbench, les manuels d'utilisation associés suivants doivent être pris en considération :

- Manuel d'utilisation du MACS TubeSealer
- Manuel d'utilisation du CliniMACS Electroporator
- Manuel d'utilisation de la CliniMACS Formulation Unit
- Manuel d'utilisation du CliniMACS Workbench

Un aperçu complet des accessoires, composants et instruments MACS GMP disponibles figure dans le manuel d'utilisation de l'instrument CliniMACS Prodigy.

Pour obtenir des informations sur les applications spécifiques, contacter le service Miltenyi Biotec Technical Support.

2
Glossaire

2.1 Niveau de danger

La couleur et le mot-indicateur d'un message d'avertissement dépendent du niveau de danger. Le niveau de danger classifie le danger comme décrit ci-dessous. Le niveau, le type et la source du danger, ainsi que les conséquences possibles, les interdictions et les mesures sont indiqués comme suit.

⚠ AVERTISSEMENT

Indique une situation dangereuse qui, si elle n'est pas évitée, pourrait entraîner des blessures graves ou la mort.

⚠ ATTENTION

Indique une situation dangereuse qui, si elle n'est pas évitée, pourrait entraîner des blessures mineures ou modérées.

REMARQUE

Indique une information considérée comme importante mais non liée à un danger (p. ex. messages concernant des dommages matériels).

IMPORTANT

Informe l'utilisateur sur des pratiques ou livre des informations importantes non liées à des blessures corporelles ni à des dommages matériels.

2.2 Conventions de présentation

Le texte en **<vert clair>** indique les éléments de l'interface graphique utilisateur (p. ex. boutons, boîtes de dialogue et éléments de gestion des utilisateurs).

2.3 Glossaire des symboles et des termes

Un aperçu des symboles et termes généraux utilisés pour le système CliniMACS Prodigy figure dans le manuel d'utilisation de l'instrument CliniMACS Prodigy. Le glossaire des symboles décrit les symboles utilisés sur l'étiquetage des Produits CliniMACS®.

2.3.1 Termes spécifiques au logiciel

Processus d'application	Logiciel de traitement cellulaire développé par Miltenyi Biotec
ATS Audit Trail System	Composant logiciel qui suit et enregistre les événements, les actions, les saisies de l'utilisateur et les modifications effectuées dans le logiciel CliniMACS Prodigy
CAP	Processus d'application personnalisé (Customized Application Process)
FTP File Transfer Protocol	Protocole de communication standard utilisé pour le transfert des fichiers informatiques d'un serveur à un client sur un réseau informatique
LDAP Lightweight Directory Access Protocol	Protocole d'application utilisé pour l'accès et la gestion de services d'information d'annuaires diffusés sur un réseau IP (Internet Protocol)
MD5	Algorithme utilisé pour générer une somme de contrôle afin de vérifier l'intégrité des données et de détecter une corruption involontaire

SMB Server Message Block	Protocole de communication utilisé pour partager des fichiers, des imprimantes, des ports en série et des communications diverses entre les nœuds d'un réseau
SMTP Simple Mail Transfer Protocol	Protocole de communication pour l'échange de courrier électronique
Processus d'application standard	Processus d'application préalablement validé fourni par Miltenyi Biotec
UMS User Management System	Composant logiciel permettant de gérer et contrôler les accès des utilisateurs à différentes fonctions de l'instrument

3 Informations importantes sur la sécurité

3.1 Consignes de sécurité pour le CliniMACS Prodigy

Pour obtenir des informations détaillées sur la sécurité de l'instrument, se reporter au manuel d'utilisation de l'instrument CliniMACS Prodigy.

3.2 Consignes de sécurité pour le logiciel

IMPORTANT

Le contrôle d'accès de l'instrument doit impérativement être validé avant utilisation. Conserver l'identifiant utilisateur et le mot de passe en lieu sûr. Il est recommandé de mettre en place un scénario d'urgence « break the glass » (voir chapitre 10 « Gestion des utilisateurs »). En cas d'échec de la connexion pendant l'exécution d'un processus, contacter le service Miltenyi Biotec Technical Support.

- Avant d'utiliser l'instrument avec la version 2.2 du logiciel, lire le chapitre 3 « Informations importantes sur la sécurité » du manuel d'utilisation de l'instrument CliniMACS Prodigy et toutes les autres informations contenues dans ce manuel d'utilisation du logiciel, y compris les consignes de sécurité et les instructions d'utilisation.
- Accorder une attention particulière à tous les avertissements affichés sur l'instrument.
- Le non-respect de ces consignes peut entraîner une utilisation inappropriée ou incorrecte et endommager l'instrument. Une utilisation incorrecte peut

également causer des blessures graves, la mort, des résultats imprévisibles, un mauvais fonctionnement de l'instrument et une usure prématurée des composants, ce qui réduit la durée de vie de l'instrument. De telles actions peuvent annuler la garantie.

- Conserver le manuel d'utilisation et toutes autres consignes de sécurité et instructions d'utilisation fournies avec l'instrument dans un endroit sûr et accessible à tous les utilisateurs pour s'y reporter ultérieurement.
- Toutes les procédures de traitement doivent être exécutées par des utilisateurs formés. L'utilisateur doit impérativement avoir une compréhension générale du traitement cellulaire ainsi que des connaissances en biosécurité.
- Seul le prestataire de services local agréé Miltenyi Biotec doit installer, entretenir ou réparer l'instrument.
- La communication et l'accès aux données entre le logiciel et le serveur/l'application externe doivent impérativement être validés avant utilisation.
- En cas de doute concernant l'utilisation en toute sécurité de l'instrument, contacter le service Miltenyi Biotec Technical Support.
- En cas de problèmes ou de défaillances, contacter le service Miltenyi Biotec Technical Support.

4

Cybersécurité

4.1 Concept de sécurité de défense en profondeur

La cybersécurité est la responsabilité commune de Miltenyi Biotec et des utilisateurs. Le logiciel est conçu avec des mesures de sécurité intégrées pour protéger contre les menaces courantes. Les utilisateurs doivent impérativement jouer un rôle actif dans la protection des données et dans le maintien de pratiques sûres. Compte tenu de l'utilisation prévue, un modèle de défense en profondeur est recommandé. Les objectifs de ce modèle de défense en profondeur sont les suivants :

- Prévention d'un impact négatif sur la qualité du produit cellulaire et d'un retard du produit cellulaire
- Intégrité des protocoles, des processus et des données d'audit
- Intégrité de la configuration du dispositif
- Disponibilité de l'instrument pour le traitement cellulaire
- Accès accordé uniquement aux utilisateurs formés et autorisés

Le modèle de défense en profondeur est structuré en couches :

- Couche de protection physique
- Couche d'environnement réseau
- Couche de logiciel de l'instrument
- Couche de l'utilisateur
- Couche d'audit
- Couche de gestion des mises à jour
- Couche de gestion de la vulnérabilité
- Couche de sauvegarde et de récupération

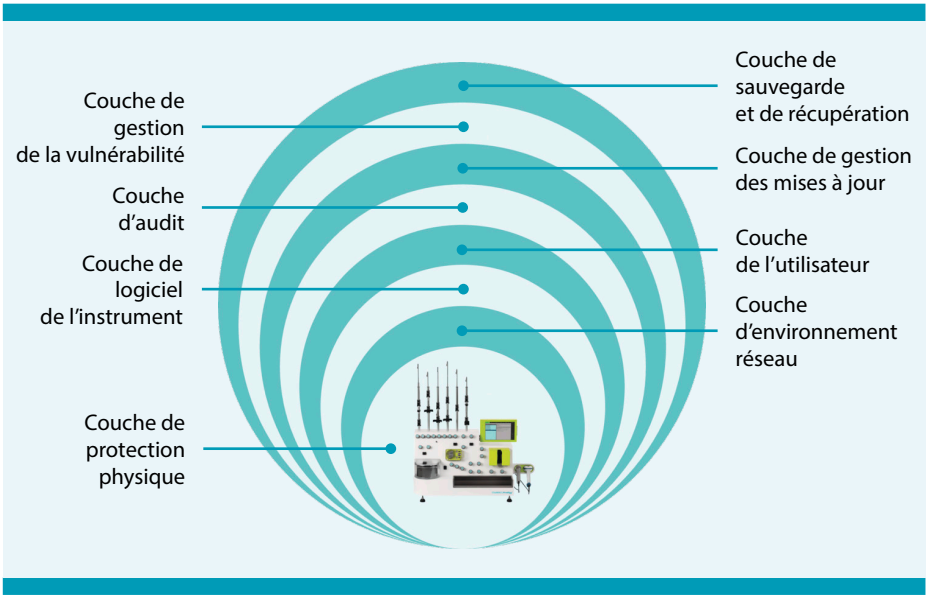


Figure 4.1: Couches du concept de défense en profondeur

4.1.1 Couche de protection physique

L'instrument est équipé des interfaces physiques suivantes qui prennent en charge la connexion des différents composants, accessoires et instruments (voir Tableau 4.1). Il est de la responsabilité du client de s'assurer que seul le personnel autorisé a un accès physique au produit et de mettre en place des procédures adaptées pour contrôler et surveiller les accès physiques.

Interface	Fonction
Port USB	Branchement des périphériques autorisés à l'instrument, par exemple le clavier externe ou le lecteur de code-barres. Un adaptateur USB Ethernet peut être utilisé pour connecter l'instrument au réseau. Des clés USB peuvent être utilisées pour le transfert de protocoles, images et fichiers journaux à partir de l'instrument et pour l'ajout de programmes/mises à jour sur l'instrument ainsi que pour son installation.
Écran tactile	Dispositif de saisie de données utilisé par le service technique et de maintenance ainsi que par les opérateurs.
Bus CAN/alimentation Interface CAN	Interface permettant de raccorder l'instrument à des dispositifs supplémentaires, comme le CliniMACS Electroporator ou la CliniMACS Formulation Unit.
Connecteur de soudeuse de tubes	Alimentation de la soudeuse MACS TubeSealer installée sur le CliniMACS Prodigy. Pas d'interface de données.
Connecteur d'alarme	Connecteur du circuit relais pour le raccordement de l'instrument à un système d'alarme externe. Pas d'interface de données.

Tableau 4.1: Interfaces et périphériques de l'instrument

Les ports USB permettent de brancher des clés USB. Même si des mesures sont en place au niveau du système d'exploitation et de l'application pour gérer les connexions USB, il est de la responsabilité du client de s'assurer que seuls des clés USB approuvées et contrôlées sont utilisées avec l'instrument.

Remarque: Seules les clés USB au format FAT32 sont prises en charge.

Une mauvaise manipulation (p. ex. force physique) des interfaces ou accessoires peut endommager les interfaces physiques de l'instrument et les rendre inexploitables, ce qui constitue un risque résiduel.

4.1.2 Couche d'environnement réseau

L'instrument doit être utilisé dans un segment de réseau protégé qui est séparé des autres segments. Un exemple de configuration dans lequel l'instrument fait partie d'un réseau d'instruments isolés est représenté à la Figure 4.2. Un routeur sépare les différents segments du réseau les uns des autres et contrôle le flux de données entre eux.

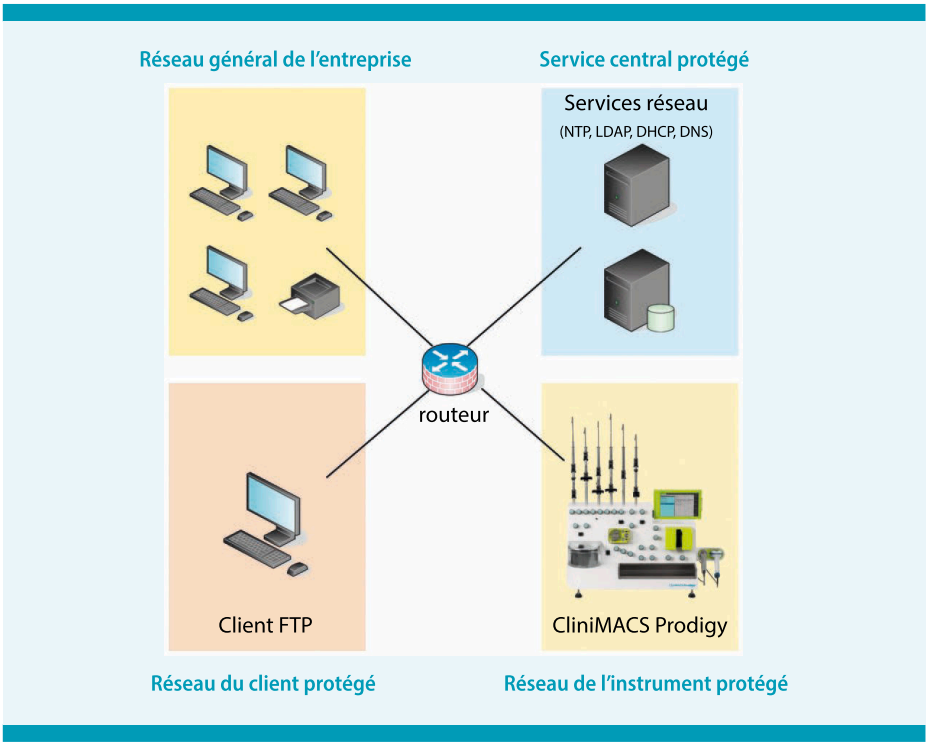


Figure 4.2: Schéma du réseau

L'instrument fournit principalement les fonctions pour se connecter aux autres systèmes du réseau. Les protocoles réseau pris en charge sont récapitulés dans le Tableau 4.2.

Interface	Fonction	Port	Commentaire
FTP	Accès au fichier journal en lecture seule via FTP	20 – 21	L'utilisation du FTP permet de transmettre les fichiers journaux et les mots de passe en texte clair sur le réseau. Il est recommandé d'utiliser un compte utilisateur dédié pour accéder aux données via FTP afin de limiter le risque pour le service FTP et de prévenir un mouvement latéral dans le cas où le compte utilisateur serait compromis. Par défaut, le protocole FTP est désactivé.
NTP	Synchronisation de l'heure	123	–
DNS (client)	Résolution de noms d'hôte en adresses IP	53 (UDP)	–

Interface	Fonction	Port	Commentaire
Demande/ réponse d'écho ICMP (serveur)	Contrôle de la connectivité du réseau vers l'instrument	N/A	–
DHCP (client)	Configuration réseau automatique de l'instrument	68 (UDP)	–
LDAP	Connexion à l'instrument avec les identifiants Active Directory gérés de manière centralisée	389	Protocole non sécurisé, à utiliser uniquement si LDAPS n'est pas pris en charge
LDAPS	Version sécurisée de LDAP	636	Variante sécurisée de LDAP. Nécessite une configuration appropriée, voir paragraphe 9.2 « Connexion à un serveur de LDAP »
SMB	Partage des fichiers	445	Le partage authentifié est pris en charge. Nécessite une configuration, voir paragraphe 9.3 « Connexion à un lecteur réseau »
SMTP	Notification par courriel	25, 2525, 465, 587	L'authentification est prise en charge. Nécessite une configuration appropriée, voir paragraphe 9.5 « Connexion à un serveur de courriel »
SMTPS	Version sécurisée de SMTP	465, 587	Variante sécurisée de SMTP. Nécessite une configuration appropriée, voir paragraphe 9.5 « Connexion à un serveur de courriel »

Tableau 4.2: Connexions et protocoles réseau

IMPORTANT

À l'exception du FTP, des protocoles sécurisés sont pris en charge pour tous les services. Il est fortement recommandé d'activer uniquement les fonctions sécurisées récapitulées dans le Tableau 4.2. Pour des raisons de compatibilité, les versions non sécurisées des protocoles sont prises en charge. Dans le cas où un protocole non sécurisé serait requis pour des raisons de compatibilité, des mesures correctives appropriées doivent impérativement être appliquées par le client.

Il est de la responsabilité du client de s'assurer que seul le personnel autorisé dispose d'un accès au réseau de l'instrument et aux réseaux utilisés pour transférer les protocoles actifs. Des processus adaptés de contrôle et de surveillance des accès au réseau doivent impérativement être en place. De plus, l'instrument ne doit en aucun cas être directement connecté à Internet.

4.1.3 Couche de logiciel de l'instrument

Un système d'exploitation Linux personnalisé est utilisé sur l'instrument. Seuls le logiciel, les services et les fonctions centrales requis sont activés pour minimiser la surface d'attaque du logiciel de l'instrument.

Seul le personnel de service formé par Miltenyi Biotec a accès au BIOS du système de l'instrument. La configuration du BIOS empêche le démarrage à partir de supports externes afin d'assurer l'intégrité du logiciel de l'instrument.

Des mesures sont en place pour garantir que seul le logiciel autorisé peut être exécuté sur l'instrument. Un nouveau logiciel est installé sur l'instrument à l'aide d'une clé USB. Le démarrage automatique du logiciel à partir de la clé USB est bloqué et un opérateur ne peut pas démarrer d'applications directement à partir d'une clé USB.

Les logiciels supplémentaires généralement disponibles sur l'instrument doivent être installés à l'aide d'un programme d'installation fourni avec ces logiciels. Pour garantir que seuls les logiciels originaux de Miltenyi Biotec prévus pour l'instrument puissent être installés, plusieurs contrôles sont en place. Plus précisément, le programme d'installation contrôle la date d'expiration du package d'installation ainsi que la signature électronique du logiciel à installer sur l'instrument. En cas d'échec d'un contrôle, le logiciel ne peut pas être installé. Avant d'exécuter l'installation, le package doit être « injecté », c'est-à-dire copié dans la mémoire volatile de l'instrument, à l'aide de l'outil Custom Files. Cet outil garantit qu'outre les formats exécutables exclusifs, seuls des fichiers originaux signés par Miltenyi Biotec peuvent être copiés sur l'instrument pour exécution.

L'installation d'une nouvelle version du logiciel de l'instrument est décrite ci-dessous au paragraphe 4.1.6 « Couche de gestion des mises à jour ».

Les nouvelles versions du logiciel de l'instrument ou le logiciel d'application personnalisé sont/est installé(es) par le service Miltenyi Biotec Technical Support.

Le système n'est pas doté d'un logiciel distinct de détection des logiciels malveillants car cela n'est pas adapté à ce produit. À la place, le risque de logiciels malveillants est contrôlé via ce concept de défense en profondeur.

Le logiciel d'application et des outils valident la plausibilité des données saisies par l'utilisateur. Cette validation comporte, entre autres, la validation des plages pour les saisies numériques, la validation des numéros de lot et de produit des consommables ainsi que des contrôles de plausibilité des données saisies.

Pendant le fonctionnement, il n'est pas demandé au logiciel et aux applications de fournir des données médicales personnelles ; il existe un faible risque qu'elles soient saisies au cours de l'exécution de l'application par l'opérateur. Il est de la

responsabilité de l'utilisateur de s'assurer que les règlementations applicables en matière de protection des données sont respectées.

Les protocoles et les données du journal peuvent être exportés à partir de l'instrument. Les données exportées sont accompagnées de l'empreinte numérique de chaque fichier permettant à l'opérateur de vérifier que l'exportation et le transfert vers un système en aval ont été exécutés avec succès et qu'aucune corruption des données ne s'est produite dans le cadre du transfert. Actuellement, l'algorithme MD5 est utilisé.

L'accès au logiciel à des fins de maintenance et aux fonctionnalités restreintes des processuss d'application est réservé au service Miltenyi Biotec Technical Support et, dans le cadre d'un fonctionnement normal, n'est pas possible pour le client. L'accès est possible pour les utilisateurs qui se connectent avec le compte de maintenance ou avec une clé USB de maintenance, c.-à-d. une clé USB contenant les informations d'authentification et le code PIN associé, ou via la fonctionnalité d'accès à distance de l'outil « Info » en combinaison avec un code PIN à usage unique fourni par Miltenyi Biotec. Seul le service Miltenyi Biotec Technical Support a accès aux identifiants du compte de maintenance et de la clé USB de maintenance. Un code PIN à usage unique peut être fourni par le support technique pour les cas d'assistance à distance.

IMPORTANT

Aucune protection n'est en place pour empêcher la lecture ou la manipulation intentionnelle des données exportées. Le client doit impérativement s'assurer que seul le personnel autorisé a accès aux données exportées.

4.1.4 Couche de l'utilisateur

Tout accès au composant peut être protégé via les paramètres de gestion des utilisateurs. Le client doit impérativement s'assurer que les instructions et recommandations décrites dans ce document sont mises en œuvre.

De plus, le client doit impérativement s'assurer que seul le personnel formé et autorisé a accès à l'instrument et que les bonnes pratiques courantes en ce qui concerne l'utilisation des mots de passe ainsi que les règlementations applicables sont respectées.

4.1.5 Couche d'audit

Le système de piste d'audit consigne les informations concernant les actions effectuées sur l'instrument, p. ex. les saisies de l'opérateur pendant l'exécution d'une application ou les modifications apportées à la configuration de l'instrument. Lorsque la piste d'audit est activée, les actions sont consignées sur la piste d'audit de l'instrument. Le client doit impérativement s'assurer que les instructions et

recommandations décrites dans ce document sont respectées.
Même si les données de piste d'audit sont générées par l'instrument, il existe un risque résiduel de mauvaise manipulation de ces données. Pour limiter ce risque, le client est responsable de la sécurité et de la manipulation des données de la piste d'audit (p. ex. exportation, stockage, suppression et révision) conformément aux règlementations applicables.

4.1.6 Couche de gestion des mises à jour

Des mises à jour de sécurité sont envoyées dans le cadre de packages de mises à jour. Miltenyi Biotec informe le client lorsqu'un nouveau logiciel est disponible.

Les mises à jour du logiciel de l'instrument doivent impérativement et uniquement être effectuées par le service Miltenyi Biotec Technical Support. Les mises à jour du logiciel de l'instrument sont fournies et installées conformément aux procédures exposées dans les SOP de Miltenyi Biotec. Les mises à jour sont regroupées dans des packages dédiés contenant le nouveau logiciel de l'instrument ainsi que le logiciel effectuant l'installation à proprement parler. Les mises à jour sont fournies sur clé USB. Pour garantir l'intégrité du package, tous les composants font l'objet d'une signature cryptographique qui est vérifiée avant l'installation. Contacter le service Miltenyi Biotec Technical Support pour planifier une mise à jour de l'instrument.

4.1.7 Couche de gestion de la vulnérabilité

Pour signaler une vulnérabilité de sécurité ou un incident impliquant le produit ou l'un de ses composants, contacter le service Miltenyi Biotec Technical Support (voir chapitre 11 « Dépannage »).

4.1.8 Couche de sauvegarde et de récupération

L'instrument est uniquement doté de la fonctionnalité de sauvegarde des protocoles et des données. Le client doit impérativement s'assurer qu'une sauvegarde de ces données est effectuée régulièrement et conformément aux règlementations applicables. Si le logiciel de l'instrument devient inexploitable, contacter le service Miltenyi Biotec Technical Support.

4.1.9 Résumé de la configuration sécurisée

Les paragraphes précédents présentent les mesures de sécurité en place et recommandent les mesures à mettre en place pour le fonctionnement en toute sécurité du CliniMACS Prodigy. Ces mesures relèvent de la configuration de l'instrument ainsi que des procédures et politiques qui renforcent la sécurité de l'instrument. Il est recommandé de prendre les mesures suivantes :

- S'assurer que seul le personnel autorisé a physiquement accès à l'instrument et à ses interfaces physiques.
- S'assurer que l'accès au réseau sur lequel l'instrument fonctionne est limité au personnel et aux systèmes autorisés.
- Activer l'authentification et l'autorisation sur chaque instrument pour s'assurer que seul le personnel autorisé peut accéder au logiciel de l'instrument.
- Le client doit impérativement avoir mis en place une gestion appropriée des autorisations pour s'assurer que le personnel utilisant ou ayant accès à l'instrument dispose uniquement des droits nécessaires à l'exécution de ses fonctions (principe du moindre privilège).
- Mettre en place une politique en matière de mots de passe qui respecte les bonnes pratiques et conforme aux règlementations applicables.
- Les protocoles sécurisés doivent être privilégiés par rapport aux alternatives non sécurisées si l'instrument les prend en charge.
- Le trafic FTP depuis et vers l'instrument n'étant pas chiffré, il est recommandé de configurer et d'utiliser un compte utilisateur dédié pour accéder aux données via le FTP.
- Des processus et procédures doivent impérativement être configurés pour garantir que seules des clés USB approuvées et contrôlées sont utilisées et empêcher l'utilisation d'autres clés USB.
- Des processus et procédures doivent impérativement être mis en place pour garantir la manipulation adéquate de la piste d'audit, des protocoles et des données du journal conformément aux règlementations applicables.
- Le personnel doit impérativement être sensibilisé aux questions de sécurité et formé à l'hygiène de base en matière de sécurité.
- Des processus et procédures doivent impérativement garantir que des sauvegardes de l'instrument sont effectuées régulièrement et conformément aux règlementations applicables.
- Il est de la responsabilité du client qu'aucune donnée médicale personnelle ne soit utilisée sur l'instrument.

5
Concept logiciel

5.1 Concept de base

Le logiciel exécuté sur l'instrument est composé du logiciel noyau et de différents logiciels d'application (ci-après les « processus d'application »). Le logiciel noyau fournit une plateforme commune pour tous les programmes exécutables, y compris les processus d'application, les outils et les paramètres.

Processus d'application

Un logiciel autonome représente un processus biologique, p. ex. un processus de transduction de lymphocytes T ou un processus d'enrichissement LP-34 Enrichment. Il contient une série d'étapes matérielles et logicielles prédéfinies afin d'automatiser le processus biologique. L'utilisateur est guidé étape par étape durant le processus. Il existe deux types de processus d'application :

- Processus d'application standard : processus d'application pré-validé fourni par défaut.
- Processus d'application personnalisé (Customized Application Process, CAP) : processus d'application développé sur mesure pour des clients spécifiques.

Outil

Programme exécutable qui peut lancer une fonction générale en dehors d'un processus d'application. Par exemple, vérifier ou modifier l'état du matériel, transférer des données, arrêter l'instrument, etc.

Paramétrage

Programme exécutable pour configurer l'instrument. Par exemple Network Settings (Paramètres réseau), Customer Settings (Paramètres client) et Module Settings (Paramètres du module)

Pour chaque programme exécutable, un dossier contenant toutes les informations est créé. Le dossier est nommé selon le modèle suivant : [Date]_[Heure]_[NuméroDeSérie]_[ProgrammeExécutable].

Le contenu de ce dossier est géré par le programme exécuté. Pour les processus d'application, les fichiers pertinents pour le client sont énumérés dans le Tableau 5.1

Nom de fichier/ dossier	Description	Format
Protocol.pdf	Enregistrement électronique de l'exécution de l'application	.pdf
Prototol_ Appendix_I.pdf	Journal des erreurs et avertissements pendant l'exécution de l'application	.pdf
Interphase	Images de la caméra des couches intermédiaires	Dossier
Microscope	Images du microscope acquises pendant l'exécution de l'application	Dossier
checksums.md5	Somme de contrôle	.md5
IR_Monitor	Consigne l'heure et la température si la température à la surface de la chambre n'est pas conforme aux spécifications pendant la culture cellulaire	.html

Tableau 5.1: Fichiers journaux des processus d'application

5.2 Interface graphique utilisateur

L'interface graphique utilisateur (GUI pour Graphic User Interface) contient plusieurs parties : barre de menu (avec menu d'accès rapide), barre d'outils, ligne d'état et zone de contenu (Figure 5.1). Pendant le fonctionnement du logiciel, les éléments et le contenu de la GUI changent en fonction de l'activité et du processus.

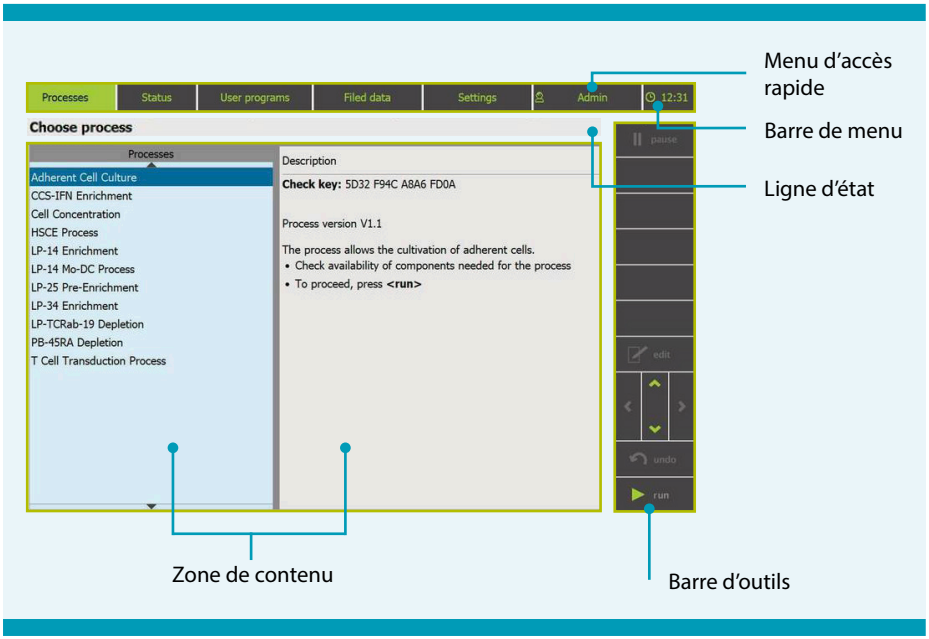


Figure 5.1: Parties de l'interface graphique utilisateur

5.2.1 Barre de menu et zone de contenu

La barre de menu permet l'accès à **<Processes>** (Processus), **<Status>** (État), **<User Programs>** (Programmes), **<Filed data>** (Données archivées), **<Settings>** (Paramètres) et (quick access menu) (menu d'accès rapide). Un arrière-plan vert indique quel bouton du menu est actif. Appuyer dans la zone correspondante pour activer le menu. La zone de contenu s'adapte en fonction du menu sélectionné. Au démarrage, le menu **<Processes>** est sélectionné par défaut et le contenu des processus s'affiche (voir Figure 5.1).

Menu	Description
<Processes> (Processus)	Accès aux processus d'application standard installés sur les instruments (Écran 6.5) et guide tout au long de l'exécution du processus (Écran 6.6)
<Status> (État)	État de l'instrument pendant l'exécution d'un processus d'application (Figure 6.1)
<User Programs> (Programmes)	Accès au Miltenyi Biotec Customized Application Process (CAP) et guide tout au long de l'exécution du processus
<Filed data> (Données archivées)	Accès à l'affichage et à l'exportation des données générées à partir des processus, des outils et des paramètres (Écran 7.1)
<Settings> (Paramètres)	Accès aux paramètres et aux outils pour la configuration de l'instrument, le test de fonctionnement et le dépannage de base (Écran 8.1)
Quick access menu (Menu d'accès rapide)	Accès aux boutons de déconnexion, de gestion des utilisateurs, de politique en matière de mots de passe, de piste d'audit et d'arrêt (Écran 6.3)
System time (Heure système)	Heure actuelle du système

Tableau 5.2: Menus de la barre de menu

5.2.2 Ligne d'état

La ligne d'état (voir Figure 5.1) contient des informations brèves sur l'état du processus en cours.

5.2.3 Barre d'outils

La barre d'outils comprend différents boutons pour le contrôle du processus. La disponibilité et l'état actif des boutons sont contrôlés par le processus d'application. La Figure 5.2 montre des exemples de barre d'outils pendant deux processus d'application différents. La couleur verte indique que le bouton est « actif » et la couleur grise qu'il est « inactif ».
Les boutons fréquemment utilisés sont expliqués dans le Tableau 5.3.

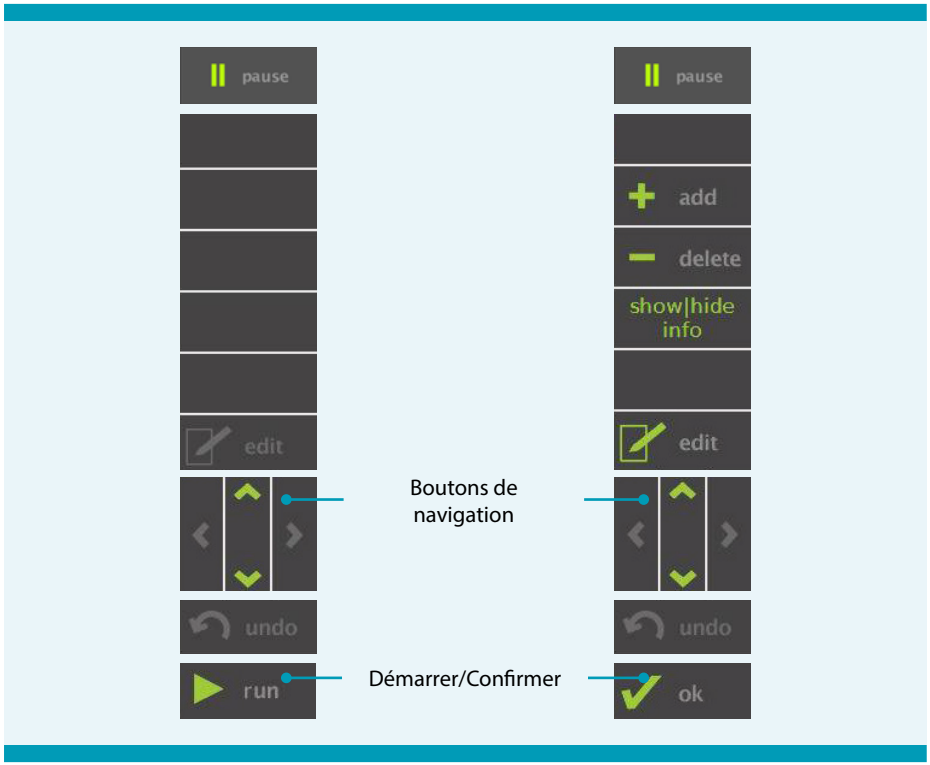


Figure 5.2: Boutons dynamiques et statiques de la barre d'outils

Bouton	Description	Disponibilité
<pause>	arrêt/interruption temporaire du processus en cours ; dépend de l'application en cours	pendant l'exécution d'un processus
<edit>	active le champ d'entrée pour permettre la saisie manuelle de données (voir 5.2.4 « Champs de saisie »).	si les champs de saisie sont disponibles
boutons de navigation	pour sélectionner des éléments dans une liste : utiliser ^ v pour déplacer l'élément sélectionné vers le haut ou vers le bas dans la liste (voir Écran 6.5) ou < > pour naviguer entre les listes (voir Écran 8.1). pour naviguer dans les images de la caméra (Figure 6.3).	toujours si la caméra est active
<undo>	annule une ou plusieurs saisie(s) pour restaurer le contenu d'origine de l'écran	pendant l'exécution d'un processus
<ok>/<run>	<ok> confirme une sélection ou ferme le menu actif <run> démarre un processus, un programme utilisateur ou toute autre procédure	toujours

Tableau 5.3: Les boutons fréquemment utilisés dans la barre d'outils

5.2.4 Champs de saisie

Un champ de saisie représente un clavier et permet la saisie de lettres ou de chiffres (voir Figure 5.3). Pour la saisie manuelle de lettres majuscules, appuyer sur <⇧>, pour la saisie d'un espace, appuyer sur <SP>, pour la saisie de chiffres, appuyer sur <?123> et pour faire un retour arrière, appuyer sur <⌫>. Pour ouvrir les champs de saisie, appuyer sur <edit> dans la barre d'outils. Pour fermer le champ de saisie, appuyer soit sur <ok> en bas du champ de saisie pour confirmer la saisie, soit sur <Escape> (Échapper) dans le coin supérieur droit pour fermer sans enregistrer.

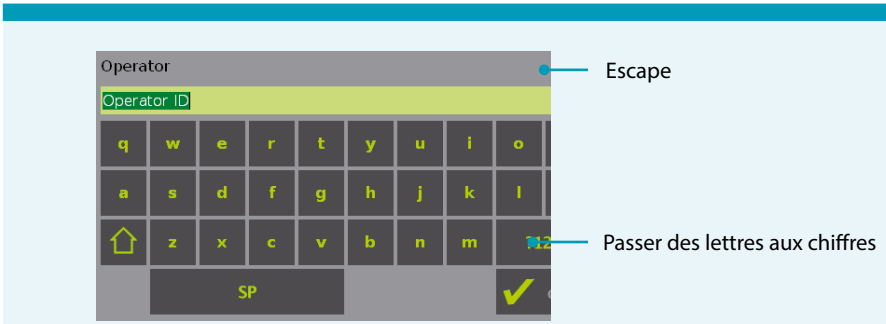
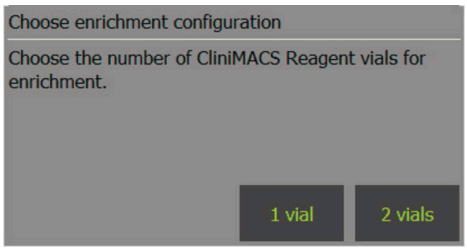


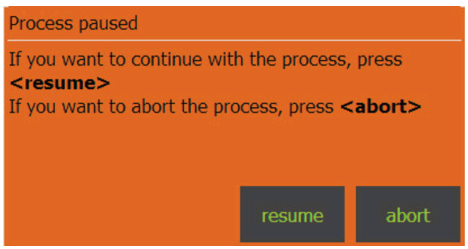
Figure 5.3: Le champ de saisie – clavier avec lettres

5.2.5 Fenêtres contextuelles

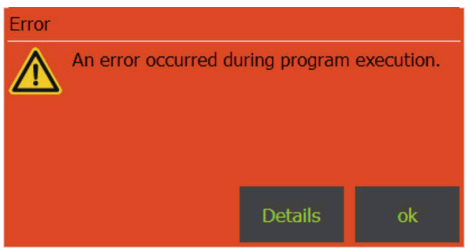
Des fenêtres contextuelles peuvent s'afficher pendant l'exécution de programmes. Le processus en cours d'exécution est alors interrompu jusqu'à la fermeture de la fenêtre contextuelle. Si nécessaire, les fenêtres contextuelles peuvent être déplacées sur l'écran en maintenant l'appui sur la barre supérieure. Une fenêtre contextuelle peut s'afficher dans différents scénarios :



Une saisie ou une confirmation est requise. La fenêtre contextuelle est grise en arrière-plan. Sélectionner l'un des boutons pour poursuivre le processus.



Un avertissement émis par l'instrument ou une décision importante nécessite une confirmation. La fenêtre contextuelle est orange en arrière-plan. Sélectionner l'un des boutons pour prendre une décision.



Une erreur s'est produite. La fenêtre contextuelle est rouge en arrière-plan. Sélectionner l'un des boutons en bas de la fenêtre pour continuer.

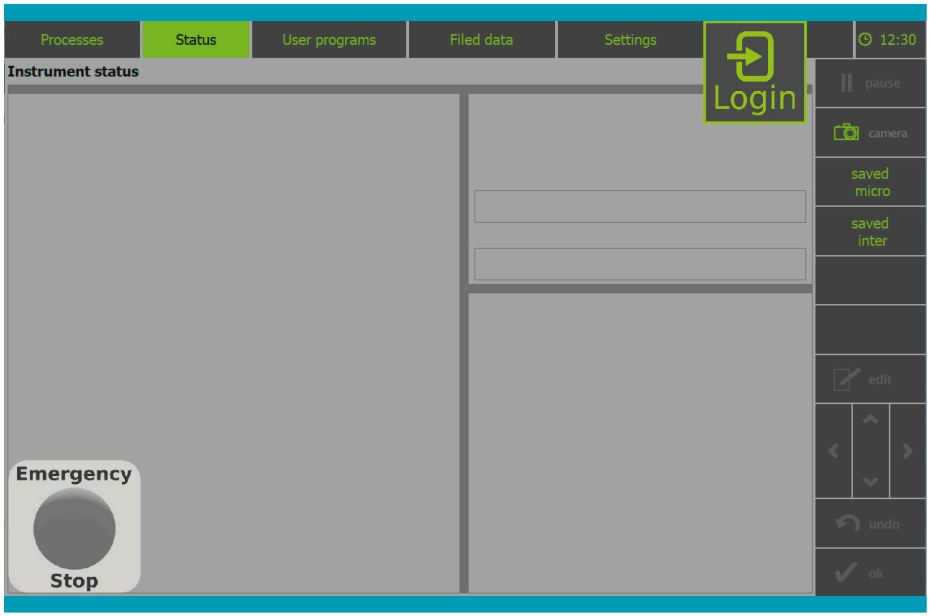
Si nécessaire, contacter le service Miltenyi Biotec Technical Support

6

Fonctionnement de base

6.1 Mise sous tension de l'instrument

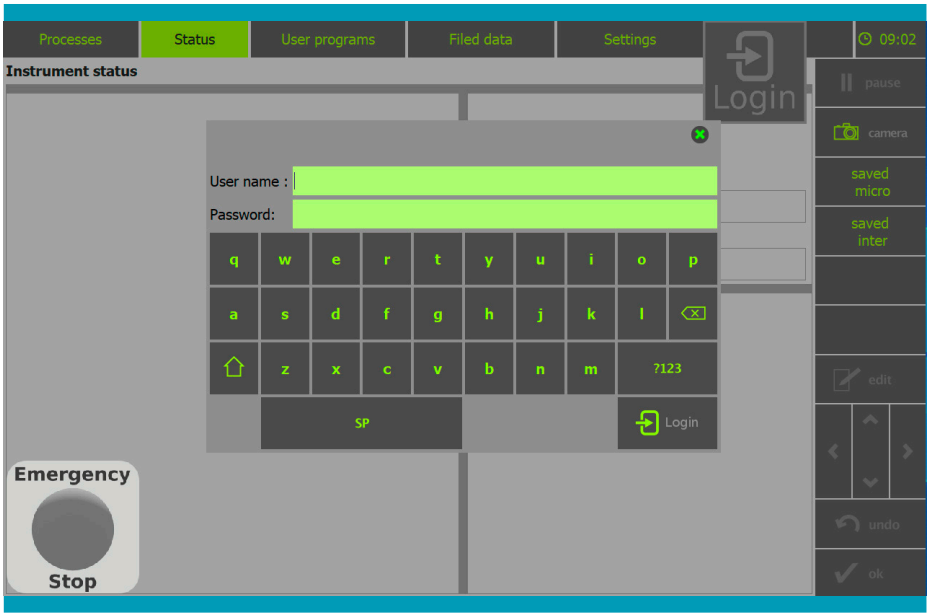
Allumer le CliniMACS Prodigy à l'aide de l'interrupteur situé à l'arrière de l'instrument. L' écran de démarrage affiche la version du logiciel et le processus d'initialisation apparaît pendant un court laps de temps (env. 5 secondes). Après le processus d'initialisation, un écran verrouillé apparaît (voir Écran 6.1). Seul le bouton **<Login>** (Connexion) est actif sur cet écran.



Écran 6.1: Écran verrouillé

6.2 Connexion

Appuyer sur <Login> dans le coin en haut à droite de l'écran pour ouvrir la fenêtre contextuelle <User Login> (Connexion de l'utilisateur, voir Écran 6.2). Saisir le nom d'utilisateur et le mot de passe, puis appuyer sur <Login> dans la fenêtre contextuelle. L'écran est alors déverrouillé. Le nom d'utilisateur et le mot de passe doivent être définis avant l'utilisation (voir chapitre 10 « Gestion des utilisateurs » pour plus de détails).



Écran 6.2: Fenêtre de connexion de l'utilisateur

Remarque: En cas d'échec de la connexion, contacter un administrateur système pour vérifier :

- L'exactitude du nom d'utilisateur et du mot de passe.
- Les droits d'accès de ce compte. Pour plus d'informations, voir le chapitre 10 « Gestion des utilisateurs ».

Si une notification contextuelle apparaît lors de la connexion et qu'elle n'est pas liée à des identifiants utilisateur incorrects ou à des droits d'accès manquants, appuyer sur <ok>. Ensuite, saisir à nouveau les identifiants utilisateur.

Contacter le service Miltenyi Biotec Technical Support si l'échec de la connexion persiste.

6.3 Logout (Déconnexion)

Appuyer sur (menu d'accès rapide) et sélectionner < Logout> dans la liste (voir Écran 6.3). L'écran est alors à nouveau verrouillé.

Remarque: Au bout de 20 minutes sans interaction avec le logiciel, l'utilisateur est automatiquement déconnecté.



Écran 6.3: Logout (Déconnexion)

6.4 Arrêt

Appuyer sur (menu d'accès rapide). Sélectionner <Shutdown> dans la liste (voir Écran 6.3). Il est également possible d'aller dans <Settings> ▸ <Tools> ▸ <Shutdown>. Attendre la fin du processus d'arrêt, puis mettre l'instrument hors tension à l'aide de l'interrupteur situé à l'arrière.

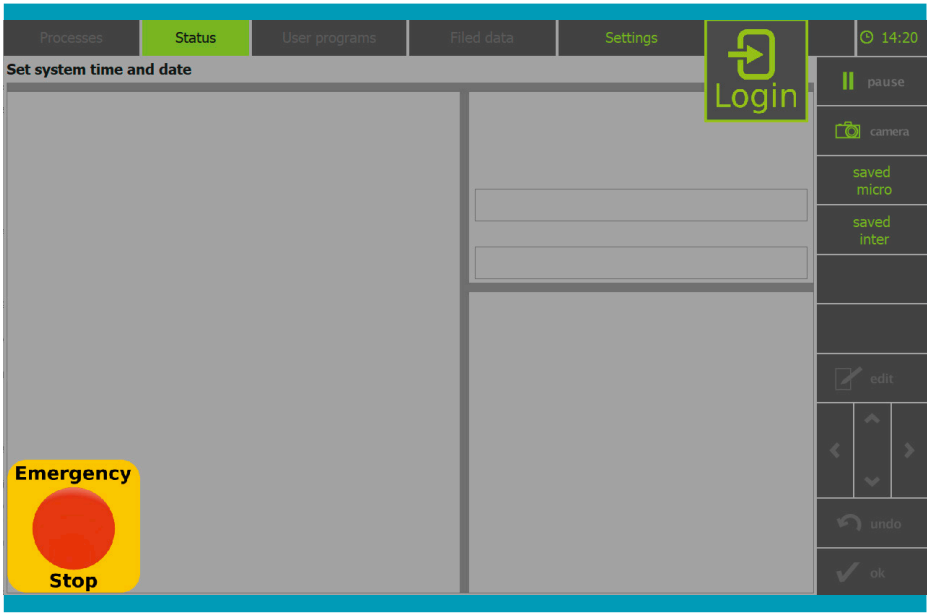
6.5 Arrêt d'urgence

Le bouton <Emergency Stop> met en pause l'application en cours d'exécution ou un outil en cas de situation d'urgence sans connexion préalable. Pour respecter les exigences de la règlementation 21 CFR Part 11, il est ensuite nécessaire de se connecter et de saisir la raison de l'arrêt d'urgence. Le bouton d'arrêt d'urgence « Emergency Stop » est uniquement activé (indiqué en jaune et rouge) lorsqu'une application ou un outil est en cours d'exécution et qu'aucun utilisateur n'est connecté (voir Écran 6.4).

IMPORTANT

Le bouton d'arrêt d'urgence <Emergency Stop> n'éteint pas complètement l'instrument car il a la même fonction que le bouton <pause> lors d'une application en cours lorsqu'un utilisateur est connecté.

Pour reprendre l'application, l'utilisateur disposant des droits nécessaires pour cette application doit se connecter.



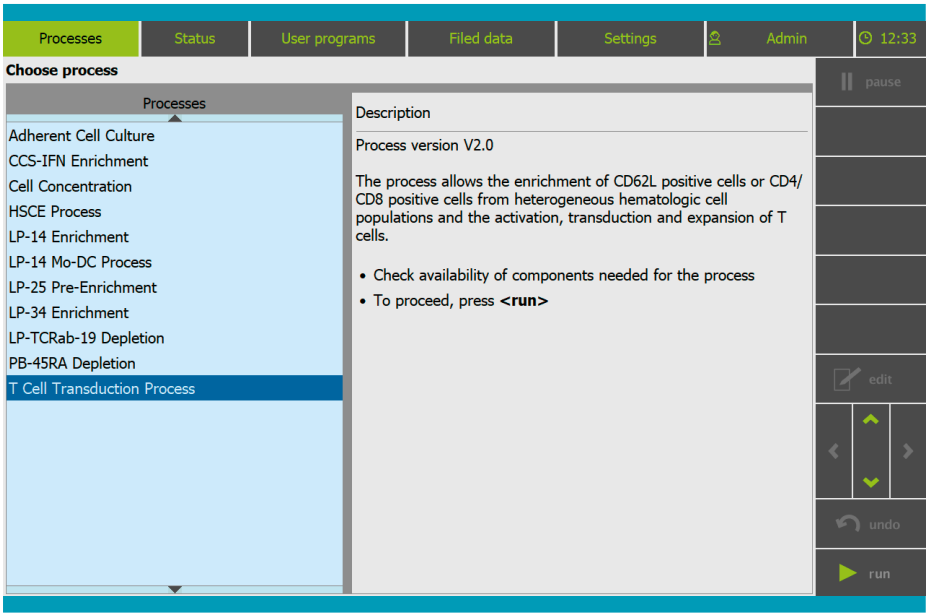
Écran 6.4: Bouton d'arrêt d'urgence

6.6 Sélectionner un processus d'application

1. Appuyer sur <Processes> (Processus) dans la barre de menu pour sélectionner un processus d'application standard. Pour un CAP, appuyer sur <User Programs> (Programmes).

2. Sélectionner le processus souhaité dans la liste des processus (Écran 6.5). Le programme sélectionné est mis en évidence avec un arrière-plan bleu. Une description de l'application est affichée à droite. Appuyer sur un processus dans la liste ou utiliser ^ et v dans la barre d'outils pour naviguer entre les processus disponibles.

Remarque: Le contenu de la liste des processus s'adapte au rôle et aux droits de l'utilisateur actuel. Une application ne s'affiche que si l'utilisateur actuellement connecté dispose des droits d'accès correspondants. Pour plus d'informations sur les rôles et les droits, voir le chapitre 10 « Gestion des utilisateurs ».



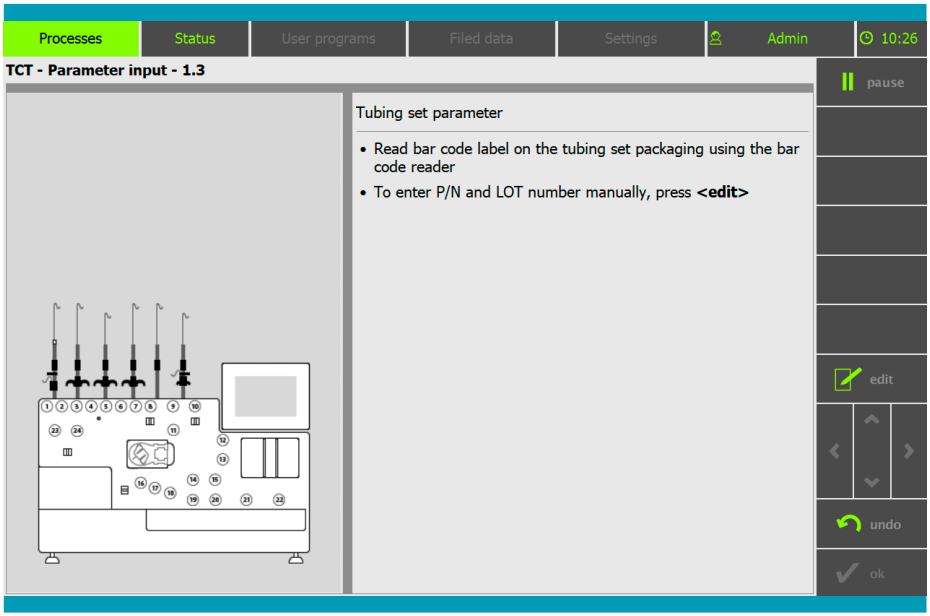
Écran 6.5: Sélectionner un processus d'application

6.7 Exécuter un processus d'application

Pour démarrer un processus, il convient de le sélectionner puis d'appuyer sur **<run>** (exécuter) dans la barre d'outils. Le logiciel fournit des instructions étape par étape tout au long du processus.
L'Écran 6.6 montre un exemple d'étape pour l'application TCT. La ligne d'état indique le nom et l'index de l'étape en cours. La zone de contenu fournit des informations complémentaires sur l'étape en question. Suivre l'illustration et les instructions dans la zone de contenu pour chaque étape.

Lors de certaines étapes de traitement, une saisie de l'utilisateur est requise. Cela concerne généralement les numéros de pièce (P/N), les numéros de lot et les valeurs de mesure. Les numéros de pièce et les numéros de lot peuvent être saisis manuellement ou avec le lecteur de code-barres. Pour la saisie manuelle ou si la valeur scannée par le lecteur de code-barres n'est pas acceptée, appuyer sur **<edit>** (modifier) dans la barre d'outils et utiliser le champ de saisie.

Lorsque toutes les actions requises sont effectuées, le bouton **<ok>** devient actif dans la barre d'outils. Pour passer à l'étape suivante, appuyer sur **<ok>**. Pour revenir à l'étape précédente, appuyer sur **<undo>** (annuler).



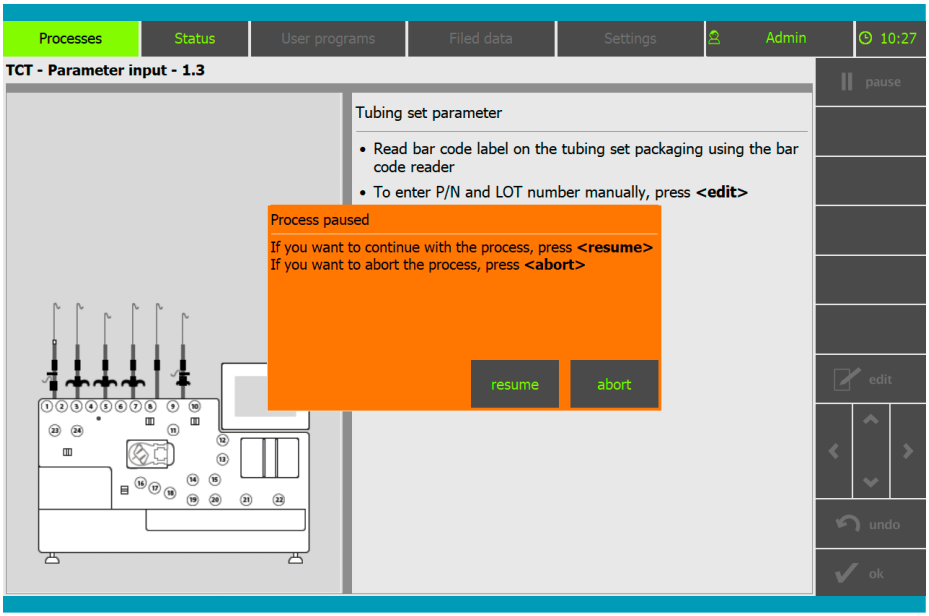
Écran 6.6: Exemple d'étape dans le processus d'application TCT

6.8 Mettre un processus d'application en pause

Pour mettre en pause le processus en cours, appuyer sur **<pause>** dans la barre d'outils. Une fenêtre contextuelle s'ouvre (Écran 6.7). Pour reprendre un processus mis en pause, appuyer sur **<resume>** (reprendre). Pour arrêter le processus, appuyer sur **<abort>** (abandonner).

IMPORTANT

Un processus abandonné ne peut pas être repris.



Écran 6.7: Processus en pause

6.9 État de l'instrument et du processus d'application

Pour vérifier l'état opérationnel du processus en cours, appuyer sur <Status> (État) dans la barre de menu. La zone de contenu affiche les éléments suivants :

- Paramètres relatifs au processus : liste de tous les paramètres pertinents du processus en cours (voir Figure 6.1 à gauche).
- Encadré d'informations et état de progression : informations relatives au processus (voir Figure 6.1, en haut à droite) :
  - Nom de l'opérateur
  - Informations sur l'échantillon
  - Progression du sous-processus et temps restant
  - Progression du processus et temps restant avant la prochaine intervention de l'utilisateur
- Aperçu graphique : fournit des informations visuelles sur l'état du sous-processus en cours d'exécution sur l'instrument (voir Figure 6.1, en bas à droite). Toutes les activités des composants de l'instrument (p. ex. pompe péristaltique, valves à pincement) sont représentées en orange.

Remarque: Les informations sur l'état sont uniquement disponibles pendant l'exécution d'une application. Cette page est vierge lorsqu'aucune application n'est en cours d'exécution. L'aperçu graphique peut ne pas être disponible pour les CAP.

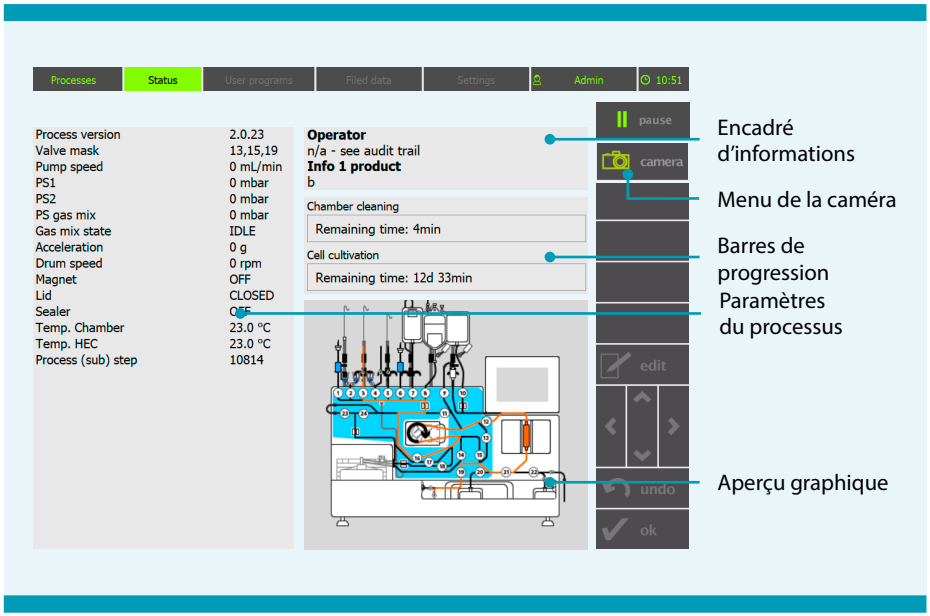


Figure 6.1: Aperçu de l'état de l'instrument

6.10 Acquisition d'images

Lors de certaines applications, deux fonctionnalités de la caméra peuvent être sélectionnées avec <camera> dans la barre d'outils (voir Figure 6.1).

- Image de la Layer Detection Camera (caméra de détection des couches) : cette image est utilisée pour mesurer les volumes des fractions de centrifugation. Elle est uniquement disponible dans certaines applications et pendant le premier ajustement du volume suivant le chargement de l'échantillon (voir Figure 6.2).
- Image microscopique : cette image peut être utilisée pour contrôler visuellement la culture cellulaire. Elle est uniquement disponible pendant les procédures de culture cellulaire (voir Figure 6.3).

L'image est automatiquement capturée et enregistrée dans le protocole par le processus d'application. Pour afficher les images, sélectionner le menu <Status> puis appuyer sur <camera> dans la barre d'outils (voir Figure 6.1). Selon l'étape du processus d'application, la zone de contenu affiche soit une image de la caméra de détection des couches soit une image microscopique.

Remarque: La disponibilité du bouton <camera> dans la barre d'outils dépend du processus d'application. Les images sont enregistrées automatiquement pendant une application.

6.10.1 Layer Detection Camera

Les différentes couches sont automatiquement détectées par le logiciel. À la Figure 6.2, les barres rouges et orange indiquent la position des couches dans l'image. Un diagramme, situé sous l'image, affiche les valeurs enregistrées pour les volumes des fractions de centrifugation. Les courbes sont affichées en rouge et en orange, en correspondance avec les barres dans l'image (voir Figure 6.2).



Figure 6.2: Aperçu de l'état de l'instrument

Les fonctionnalités suivantes sont disponibles :

- Enregistrement d'image : appuyer sur <snap> (photo) dans la barre d'outils. Après une courte phase d'enregistrement (env. 15 secondes), l'image affichée est remplacée par l'image nouvellement enregistrée.
- Archivage d'image : appuyer sur <save > (sauvegarder) dans la barre d'outils. L'image enregistrée sera intégrée au protocole du processus actuel.
- Sortie du menu de la caméra : appuyer sur <ok> dans la barre d'outils.

Remarque: La disponibilité des boutons ci-dessus dépend du processus d'application.

6.10.2 Caméra microscope

Le menu de la caméra montre la dernière image sauvegardée par la caméra microscope intégrée (voir Figure 6.3).

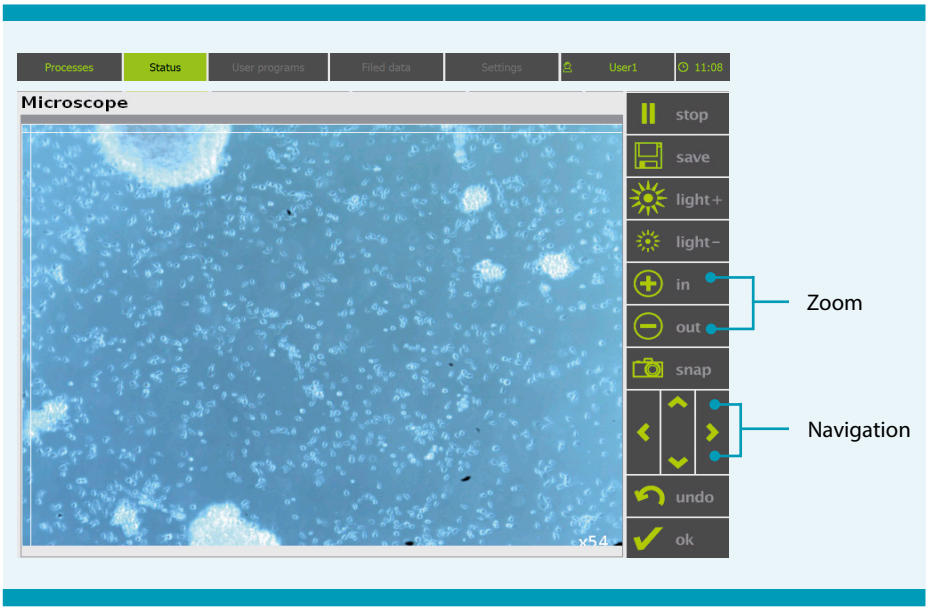


Figure 6.3: Écran d'état lorsque la caméra microscope est active

Les fonctionnalités suivantes sont disponibles :

- Aggrandir l'image : Toucher l'image de la caméra microscope pour l'agrandir deux fois. Le point de contact devient le nouveau centre de l'image. Il est possible d'agrandir les images jusqu'à 400 fois.
- Navigation dans une image : Appuyer sur un bouton de navigation pour déplacer l'image d'une demie vue dans la direction sélectionnée. Les barres de défilement montrent la position absolue de la section affichée dans l'ensemble de l'image afin de faciliter la navigation. Appuyer plusieurs fois sur **<undo>** (annuler) pour annuler une à une les dix dernières actions de navigation.
- Enregistrement d'image : appuyer sur **<snap>** (photo) dans la barre d'outils. Après une courte phase d'enregistrement (env. 15 secondes), l'image affichée est remplacée par l'image nouvellement enregistrée.
- Archivage d'image : appuyer sur **<save >** (sauvegarder) dans la barre d'outils. L'image enregistrée sera intégrée au protocole du processus actuel.
- Sortie du menu de la caméra : pour quitter le menu de la caméra, appuyer sur **<ok>** dans la barre d'outils.

Remarque: La disponibilité des boutons ci-dessus dépend du processus d'application.

7 Accès aux données

7.1 Récupération des journaux d'application

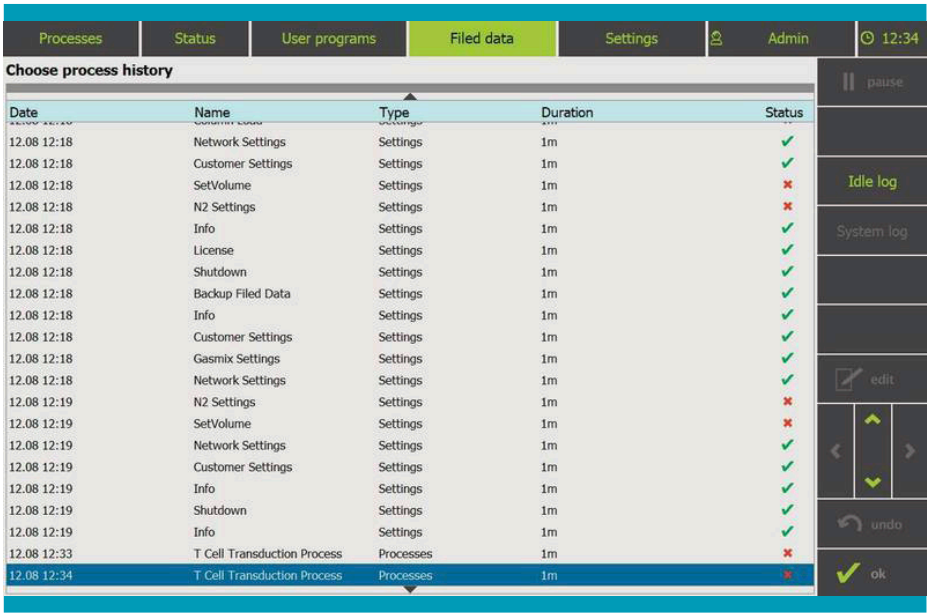
7.1.1 Affichage et exportation des fichiers journaux vers une clé USB

Le menu **<Filed data>** (Données archivées) affiche le fichier journal généré à partir des processus d'application, des outils et des paramètres. Dans la zone de contenu, la liste des fichiers indique l'heure, le nom, le type, la durée et l'état de l'exécution du processus (Écran 7.1).

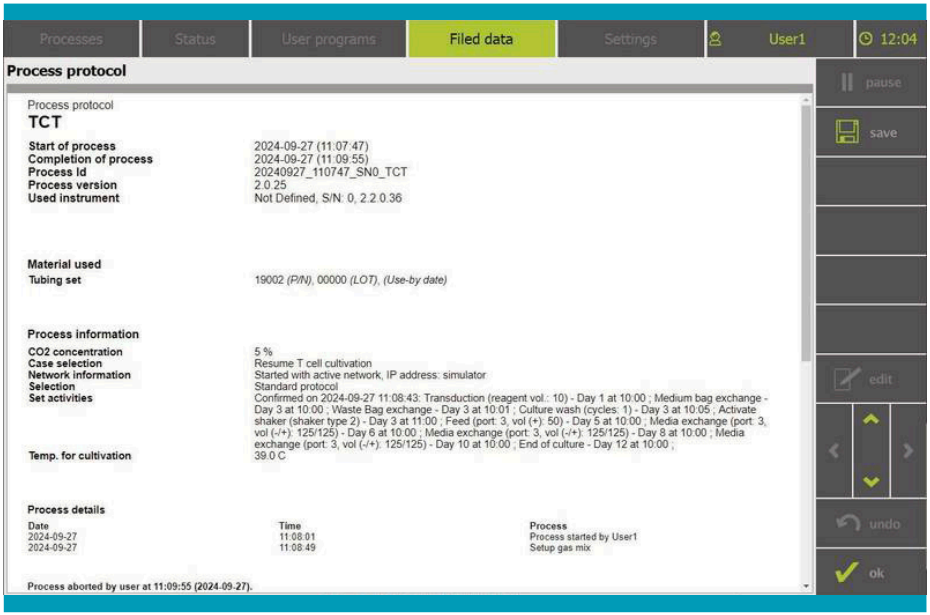
Remarque: Le menu **<Filed data>** n'est pas disponible durant l'exécution d'un processus. Le bouton tactile correspondant est inactif.

Affichage des fichiers journaux

Pour afficher le contenu du PDF du protocole du processus et du PDF des annexes du protocole, sélectionner le fichier journal souhaité et appuyer sur **<ok>** (voir Écran 7.1). Le contenu du fichier sélectionné s'affiche alors dans la zone de contenu (voir Écran 7.2). Pour revenir à la liste des fichiers, appuyer sur **<ok>**.



Écran 7.1: Exemple de liste de données archivées



Écran 7.2: Exemple d'un protocole de processus (application TCT)

Exportation vers une clé USB

1. Insérer une clé USB.
2. Ouvrir le fichier journal souhaité et appuyer sur <save> (sauvegarder) dans la barre d'outils.

IMPORTANT

- Vérifier que le nom de la clé USB n'est pas « netext » car ce nom est réservé au logiciel.
- Pour sauvegarder toutes les données d'un processus, il est possible d'utiliser l'outil Backup Filed Data (Sauvegarde des données archivées), voir paragraphe 8.2.2 « Backup Filed Data (Sauvegarde des données archivées) ».
- La clé USB doit impérativement être au format FAT32 et ne doit pas être protégée par un mot de passe.

7.1.2 Récupération via FTP

FTP est un protocole de réseau qui permet le transfert de données entre le CliniMACS Prodigy (appelé le serveur FTP) et l'ordinateur de l'utilisateur final (appelé le client FTP) par le biais de connexions IP (Internet Protocol). Il est possible d'accéder à tous les fichiers journaux générés durant l'exécution de l'application.

Pour accéder aux données via FTP, il est nécessaire de procéder à une configuration. Pour configurer l'instrument pour une connexion FTP, suivre les instructions du paragraphe 9.4.1 « Paramétrage de l'instrument ». Après la configuration, l'utilisateur peut se connecter à l'instrument avec tout client FTP disponible (p. ex. FileZilla) afin de télécharger les protocoles et les fichiers journaux, Figure 7.1 montre un exemple de paramètres de connexion. Pour se connecter à l'instrument, saisir les informations suivantes :

- Adresse IP de l'instrument. Elle figure dans <Settings> ▸ <Tools> ▸ <Info> ▸ <Network information>.
- Port : utiliser un port 21 standard.
- Pour le nom d'utilisateur et le mot de passe, deux options de connexion sont prises en charge :
    - Option de connexion 1 : un compte enregistré dans le système de gestion des utilisateurs (voir chapitre 10 « Gestion des utilisateurs »). Dans ce cas, utiliser le compte et le mot de passe de connexion de l'utilisateur. L'établissement et l'interruption de la connexion seront consignés sur la piste d'audit.
    - Option de connexion 2 : un nom d'utilisateur local et le mot de passe associé enregistrés dans FTP/paramètres de partage des fichiers. Les informations

de connexion figurent dans <Settings> ▸ <Network Settings> FTP/FS. Dans ce cas, l'établissement et l'interruption de la connexion ne seront pas consignés sur la piste d'audit.

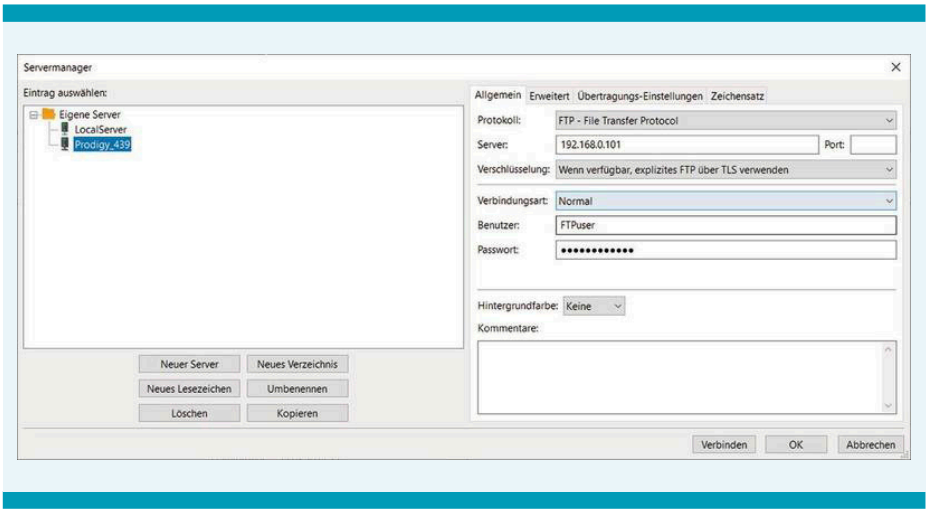


Figure 7.1: Exemple de paramètres de connexion

IMPORTANT

- Si l'option de connexion 1 est utilisée, vérifier que le rôle « File management user » (Utilisateur des outils de gestion de fichiers) est attribué à ce compte. Pour savoir comment attribuer ce rôle au compte, consulter le chapitre 10 « Gestion des utilisateurs ».
- Le logiciel ne prend pas en charge le protocole FTP sécurisé (sFTP). Il est recommandé d'utiliser l'instrument sur un réseau séparé si l'accès aux fichiers se fait via FTP.

Remarque: Un utilisateur individuel peut établir une seule connexion à la fois car les connexions multiples ne sont pas autorisées par le serveur de l'instrument. Si un logiciel client qui utilise des connexions simultanées est utilisé (p ex. FileZilla), modifier les paramètres du client en conséquence pour n'autoriser qu'une seule session. Si cela n'est pas fait, le contenu peut être parcouru mais pas téléchargé.

7.1.3 Récupération des fichiers via le partage des fichiers

Les fichiers journaux générés pendant l'exécution de l'application peuvent être récupérés via un dossier réseau partagé. Une fois l'exécution de l'application terminée, tous les fichiers générés sont automatiquement placés dans un sous-dossier créé pour chaque instrument dans le dossier partagé.
Figure 7.2 montre la structure des fichiers dans le dossier partagé. Pour activer le partage des fichiers, il est nécessaire de procéder à une configuration. Pour

configurer le partage des fichiers, suivre les instructions au paragraphe 9.3 « Connexion à une unité du réseau ».

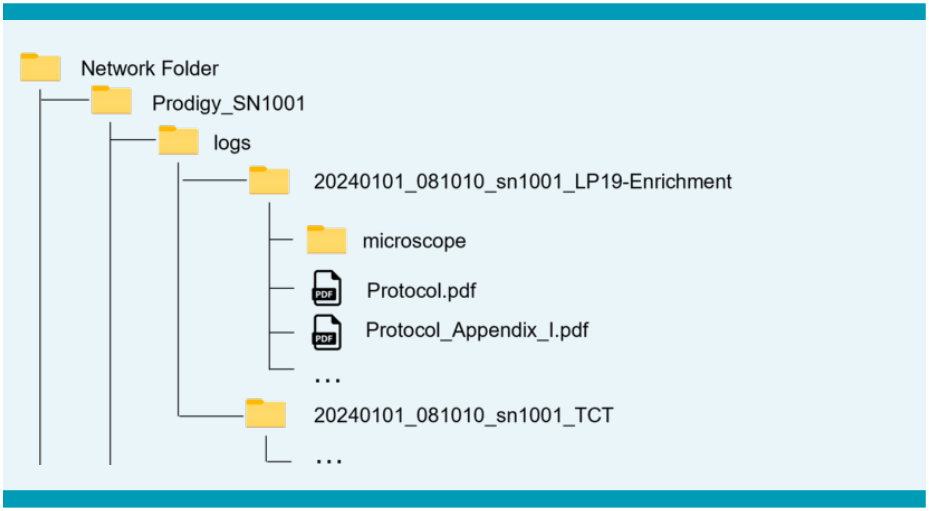


Figure 7.2: Structure de fichiers dans le partage des fichiers

IMPORTANT

Les fichiers journaux stockés sur l'instrument sont protégés par un contrôle d'accès qui réserve l'accès au personnel autorisé. Une fois que ces fichiers sont transférés sur un lecteur réseau, il est de la responsabilité de l'utilisateur de mettre en place les mesures de contrôle d'accès appropriées.

7.2 Récupération de piste d'audit

Le système de piste d'audit enregistre toutes les interactions de l'utilisateur avec le logiciel. Chaque intervention de l'utilisateur génère un enregistrement sur la piste d'audit incluant l'utilisateur en question, l'estampille temporelle et la description de l'intervention. La piste d'audit peut être exportée au format .pdf ou .csv. Le Tableau 7.1 montre le format de la piste d'audit.

IMPORTANT

L'estampille temporelle de l'enregistrement sur la piste d'audit est toujours dans le fuseau horaire UTC.

Heure	Catégorie	Type	Utilisateur	Description
2020-Jul-21 10:33:44	Intervention de l'utilisateur	Fermeture de la fenêtre contextuelle	IdentifiantCompte	« Avertissement » progression en pause
...	...	...	...	...

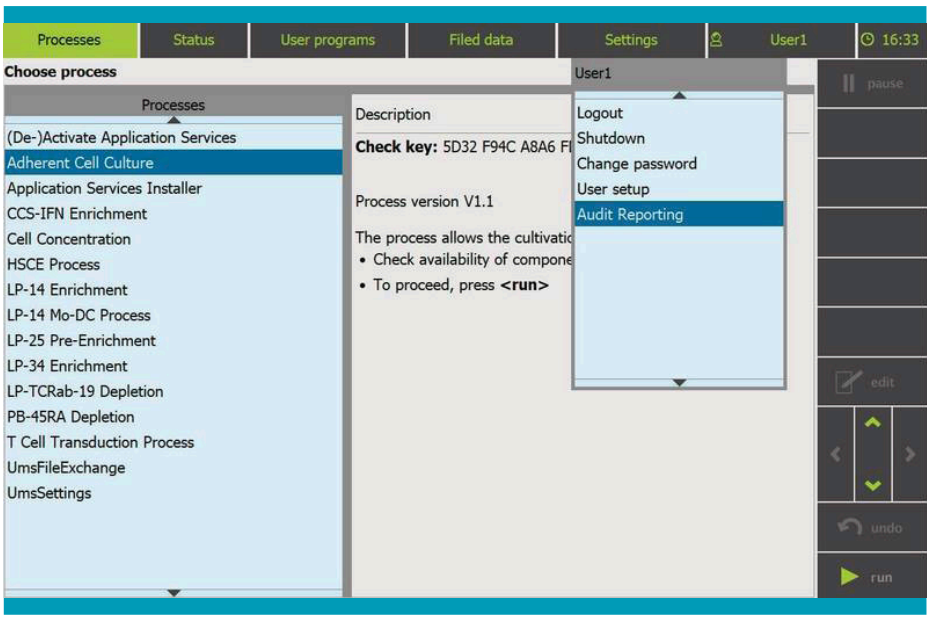
Tableau 7.1: Format de piste d'audit

Remarque: Le rôle « ATS User » (Utilisateur ATS) ou un rôle disposant des droits « Audit Trail Management » (Gestion de la piste d'audit) est requis pour accéder au système de la piste d'audit.

- Le rôle « ATS User » dispose d'un accès total qui permet d'afficher, d'exporter et de supprimer les enregistrements de la piste d'audit.
- Un nouveau rôle peut être créé pour un accès limité aux fonctions de la piste d'audit. Voir le chapitre 10 « Gestion des utilisateurs » pour plus de détails sur la manière de configurer les rôles et les droits.

7.2.1 Affichage de la piste d'audit

Pour ouvrir la piste d'audit, aller dans ▸ <Audit Reporting> (Rapport de vérification) (voir Écran 7.3). Le menu <Audit Trail> contient une liste de tous les événements disponibles sur la piste d'audit de l'instrument (voir Écran 7.3).



Écran 7.3: Rapport de vérification

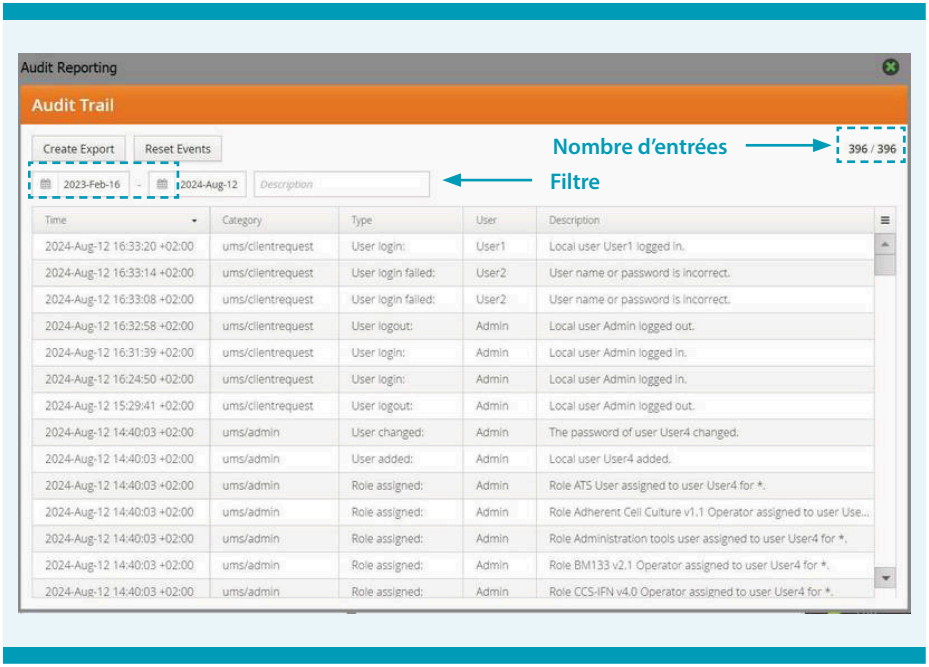
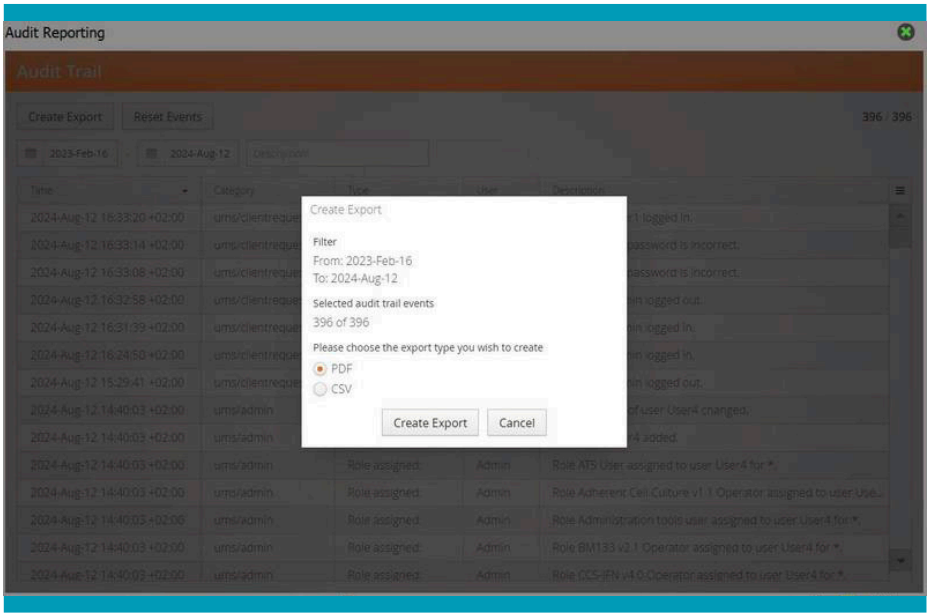


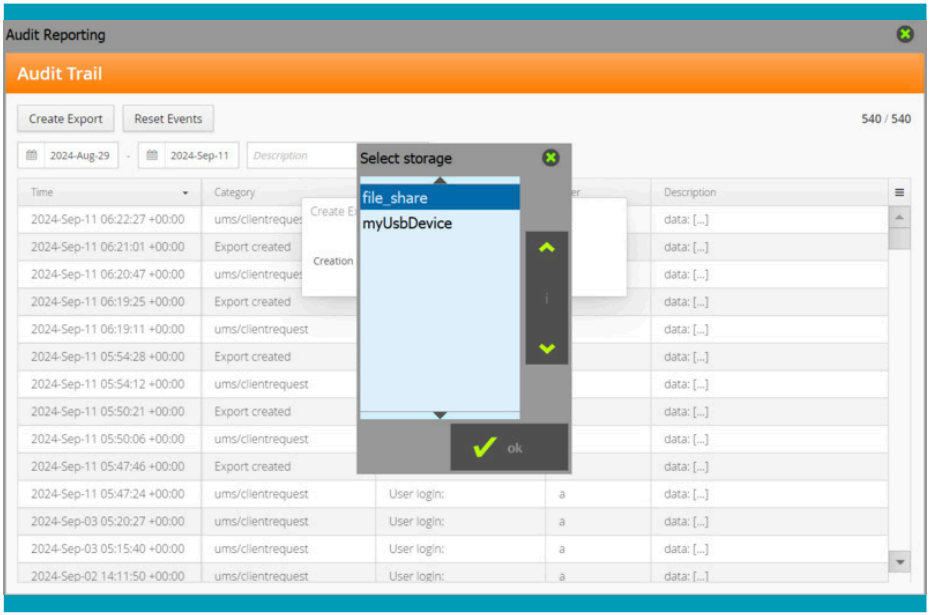
Figure 7.3: Menu « Audit Trail »

7.2.2 Exportation de la piste d'audit

1. Saisir les critères de filtrage dans les champs comme à la Figure 7.3. Si aucun critère n'est saisi, tous les enregistrements de la piste d'audit seront exportés.
2. Appuyer sur **<Create Export>** (Créer un exportation) au-dessus des critères de filtrage. Une fenêtre contextuelle s'ouvre (voir Écran 7.4).
3. Choisir le format et appuyer sur **<Create Export>** dans la fenêtre contextuelle.
4. Si plusieurs emplacements de stockage sont détectés, p. ex. si le partage des fichiers est configuré et si une clé USB est insérée, l'emplacement de stockage doit être défini (voir Écran 7.5).



Écran 7.4: Créer une exportation de piste d'audit



Écran 7.5: Sélectionner l'emplacement de stockage de la piste d'audit

5. Patienter jusqu'à la fin du processus et vérifier si le fichier a bien été exporté.

7.2.3 Suppression de la piste d'audit

1. Pour supprimer toutes les entrées de la piste d'audit, appuyer sur **< Reset Events >** (Réinitialiser les événements).

2. Confirmer en appuyant sur **<Continue Reset>** (Poursuivre la réinitialisation). Après la réinitialisation, tous les enregistrements sont supprimés. Un nouvel enregistrement pour l'action de suppression est ajouté.

IMPORTANT

Il n'est pas possible de supprimer les entrées individuellement. Les données supprimées ne peuvent pas être restaurées. S'assurer que seuls les utilisateurs autorisés ont le droit de supprimer la piste d'audit. Pour configurer les rôles et les droits, voir le chapitre 10 « Gestion des utilisateurs ».

8

Outils et paramètres utilisateur

8.1 Accès aux outils et paramètres utilisateur

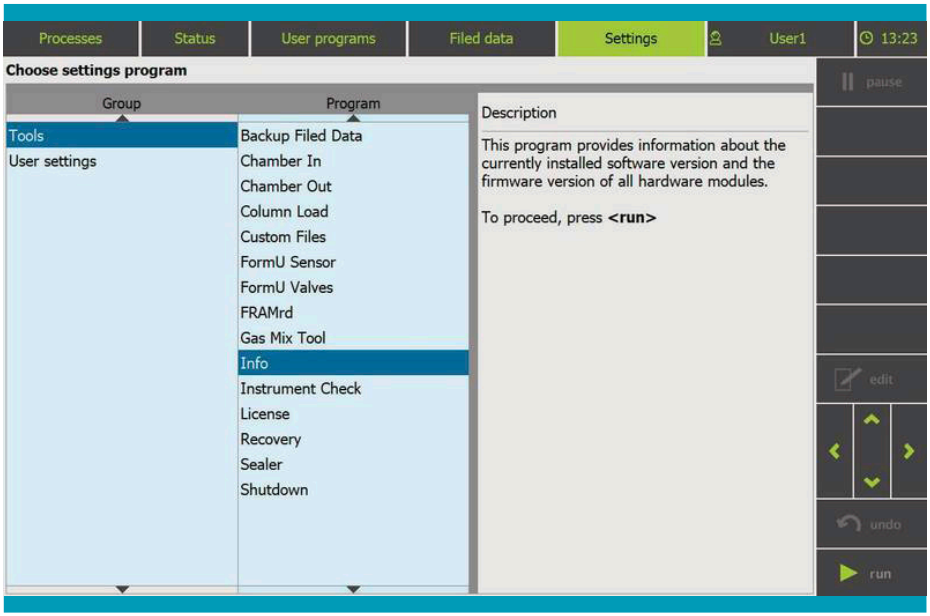
Deux types de programmes figurent dans le menu **<Settings>** : les outils et les paramètres.

Remarque: Les outils et les paramètres ne sont pas disponibles pendant l'exécution d'un processus.

Pour trouver et exécuter un outil/paramètre :

1. Sélectionner **<Tools>** ou **<User settings>** dans la liste des groupes (voir Écran 8.1).
2. Appuyer sur le programme souhaité dans la liste des programmes. Le programme sélectionné est mis en évidence avec un arrière-plan bleu. Des informations détaillées sur l'outil/le paramètre sélectionné figurent dans le champ de description. Appuyer sur ^ et v au dessus et en dessous de la liste des programmes pour voir plus d'options. Il est également possible d'utiliser les boutons de navigation pour naviguer parmi les programmes et sélectionner le programme souhaité.
3. Pour démarrer le programme sélectionné, appuyer sur **<run>** dans la barre d'outils.

Les outils et paramètres utilisateur couramment utilisés sont présentés dans les paragraphes qui suivent.



Écran 8.1: Sélection d'un outil ou d'un paramètre

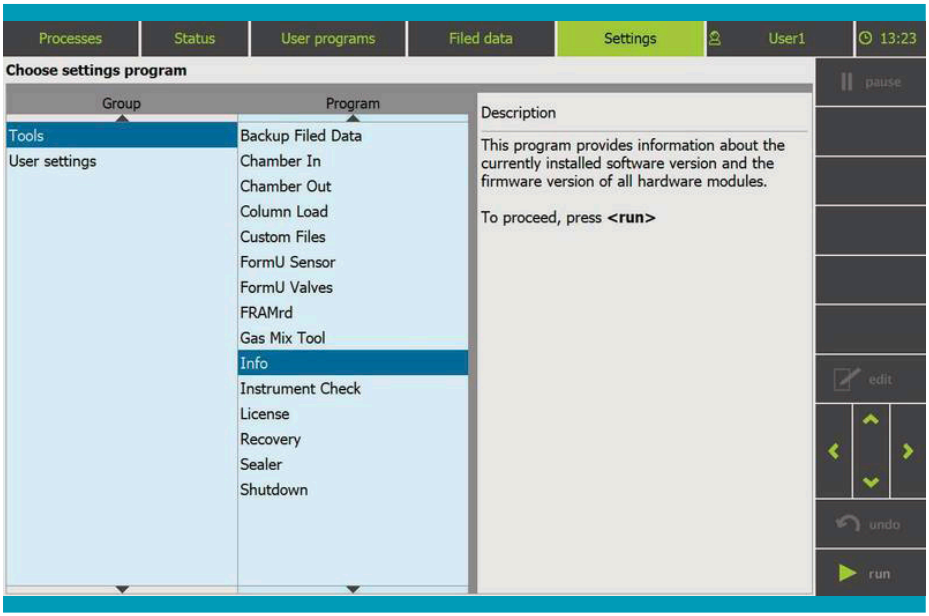
8.2 Tools (Outils)

Tous les outils figurent sous **<Settings>** ▸ **<Tools>**.

8.2.1 Info tool (Outil Info)

L'outil Info fournit des informations détaillées sur le logiciel et le matériel. Les informations importantes sont les suivantes :

- Version du logiciel
- Numéro de version
- Version du micrologiciel
- Utilisation de l'espace du disque dur, y compris espace restant, espace utilisé et espace total
- Adresse IP
- Adresse MAC
- Informations complètes sur la durée d'activité (y compris toutes les applications et tous les outils), durée d'inactivité (durée pendant laquelle l'instrument n'exécutait aucune application)



Écran 8.2: Outil Info

8.2.2 Backup Filed Data (Sauvegarde des données archivées)

L'outil Backup Filed Data copie toutes les données du processus vers un emplacement de sauvegarde ou les supprime toutes.

IMPORTANT

- Il est recommandé de sauvegarder régulièrement les données de processus. Autrement, un message d'invite utilisateur peut s'afficher, indiquant que le programme ne doit pas être lancé car la limite de données archivées a été atteinte.
- Si une clé USB est utilisée pour la sauvegarde, cette clé doit impérativement être de type FAT 32 et ne doit pas être protégée par un mot de passe.
- Si le partage des fichiers est configuré, les fichiers peuvent également être exportés vers le dossier de partage des fichiers (voir paragraphe 9.3 « Connexion à une unité du réseau »).

Copie de données

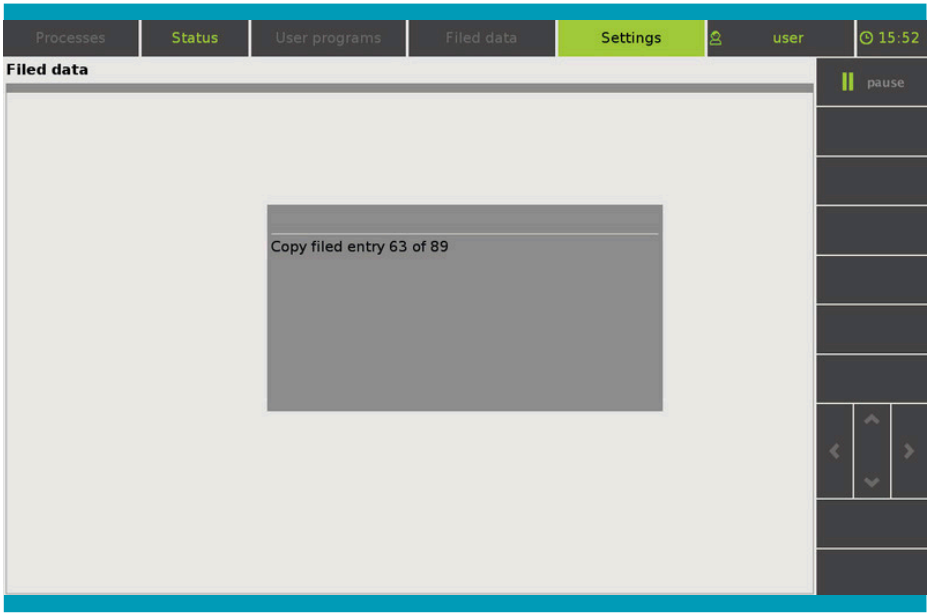
1. Insérer une clé USB.

2. Aller dans <Settings > ▸ <Tools> ▸ <Backup Filed Data>, et appuyer sur <run>.

3. Sélectionner <Backup> dans la fenêtre contextuelle (voir Écran 8.3). La copie démarre (voir Écran 8.4).

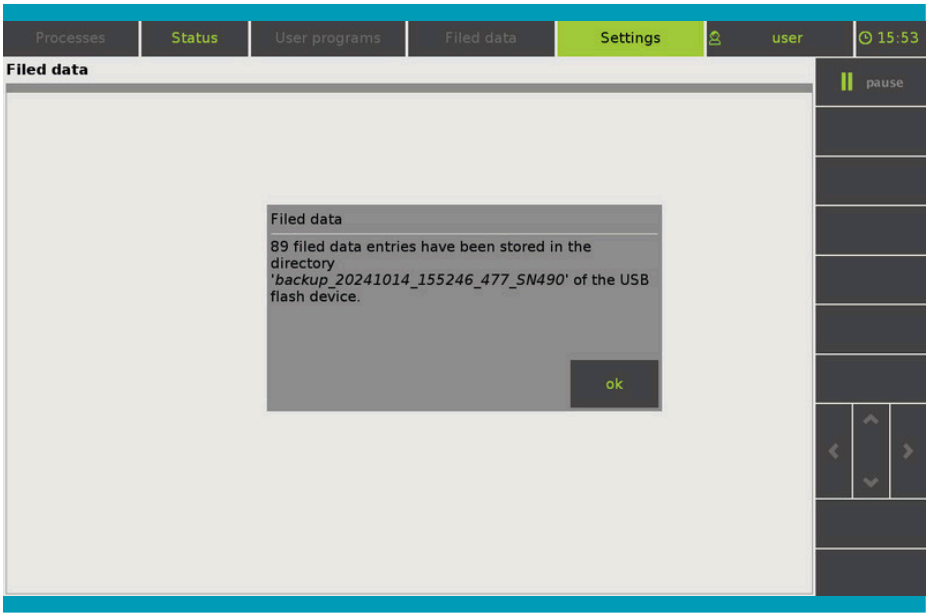


Écran 8.3: Sélectionner Backup



Écran 8.4: Processus de sauvegarde

4. Patienter jusqu'à ce que la copie soit terminée, puis appuyer sur <ok> dans la fenêtre contextuelle (voir Écran 8.5).
5. Vérifier que tous les fichiers ont été téléchargés intégralement.



Écran 8.5: Sauvegarde terminée

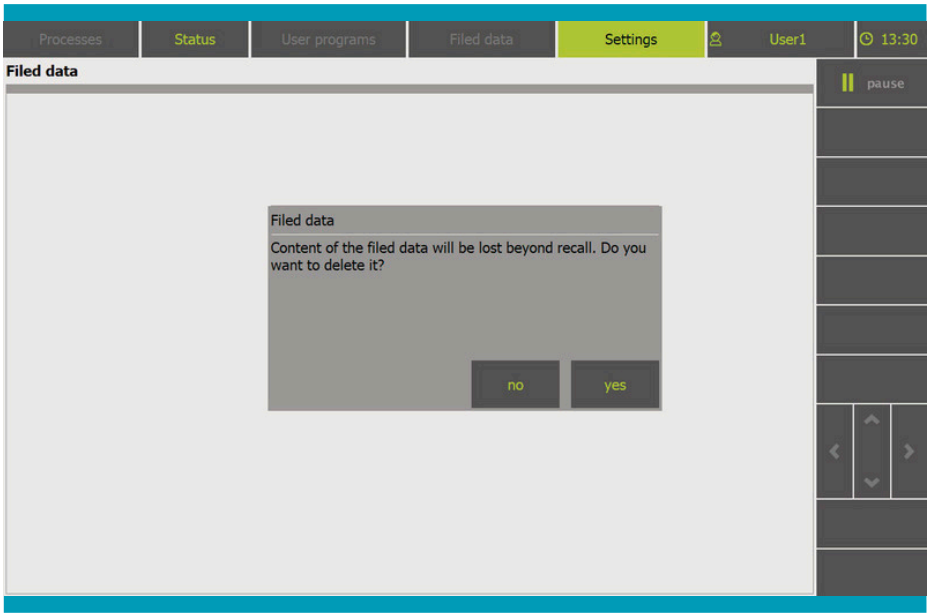
Suppression des données

1. Vérifier que tous les fichiers ont été téléchargés intégralement.
2. Aller dans **<Settings >** ▸ **<Tools>** ▸ **<Backup Filed Data>**, et appuyer sur **<run>**.
3. Appuyer sur **<Delete>** (Supprimer) (voir Écran 8.6).



Écran 8.6: Sélectionner Delete

4. Pour confirmer, appuyer sur <yes> (oui) (voir Écran 8.7).



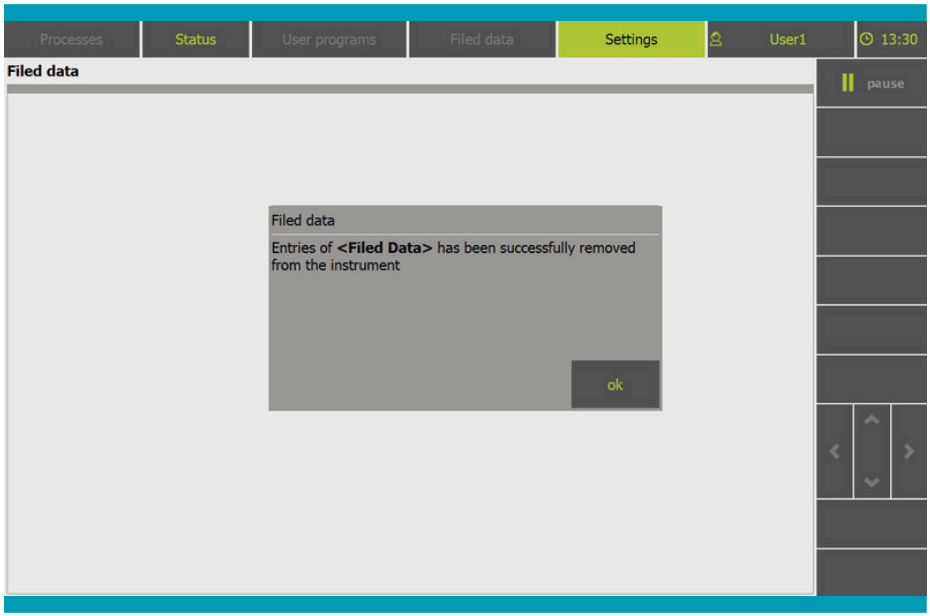
Écran 8.7: Confirmer la suppression des données

5. Patienter jusqu'à la fin de la suppression, puis appuyer sur **< ok >** dans la fenêtre contextuelle (voir Écran 8.8).

6. Après la suppression, tous les enregistrements sont supprimés de **<Filed Data>** (Données archivées). Un enregistrement est créé pour l'exécution de l'outil Backup Filed Data.

IMPORTANT

Les données supprimées ne peuvent pas être restaurées.



Écran 8.8: Suppression terminée

8.2.3 Chamber In (Insertion de la chambre)

Cet outil est utilisé pour insérer l'unité CentriCult en dehors d'une application en cours d'exécution. L'adaptateur de verrouillage de la chambre se déplace vers la position d'insertion et déverrouille le couvercle de l'unité CentriCult. Après l'exécution de cet outil, ouvrir l'unité CentriCult manuellement.

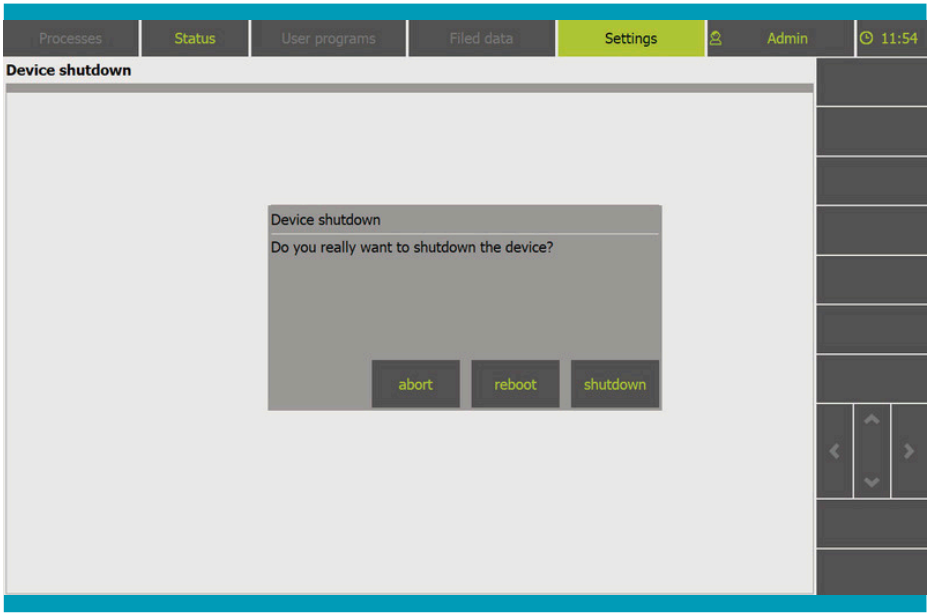
8.2.4 Chamber Out (Retrait de la chambre)

Cet outil est utilisé pour retirer l'unité CentriCult en dehors d'une application en cours d'exécution. L'adaptateur de verrouillage de la chambre se déplace vers la position de retrait et déverrouille le couvercle de l'unité CentriCult. Après l'exécution de cet outil, ouvrir l'unité CentriCult manuellement.

8.2.5 Shutdown (Arrêt)

Cet outil permet d'arrêter ou de redémarrer l'instrument.

1. Appuyer sur <run> dans la barre d'outils pour exécuter la fonction d'arrêt.
2. Sélectionner < abort > (abandonner), <shutdown > (arrêt) ou < reboot > (redémarrer) (voir Écran 8.9).



Écran 8.9: Sélectionner shutdown (arrêt) ou reboot (redémarrer)

8.2.6 Recovery (Récupération)

Ce programme permet le sauvetage de produits cellulaires dans des poches prévues à cet effet en cas d'échec du processus. Cet outil prend uniquement en charge les jeux de tubulures CliniMACS Prodigy suivants : TS 310, TS 500 et TS 510.

IMPORTANT

Utiliser uniquement cet outil sur instruction du service Miltenyi Biotec Technical Support.

8.2.7 Gas Mix tool (Outil pour mélange des gaz)

Ce programme permet de prélever du gaz avec une poche d'échantillonnage à partir de l'unité de mélange des gaz.

8.2.8 Instrument Check (Contrôle de l'instrument)

Cet outil effectue un contrôle semi-automatisé de l'instrument nécessitant certaines interventions de l'utilisateur.

8.2.9 Column Load (Chargement des colonnes)

Dans certains cas spécifiques, le processus permet l'enrichissement des cellules CD34 positives à partir de produits de leucaphérèse.

8.2.10 Custom Files (Fichiers personnalisés)

Ce programme est utilisé pour ajouter des CAP à l'instrument.

8.2.11 Sealer (Soudeuse)

Ce programme est utilisé pour allumer/éteindre la soudeuse (Sealer).

8.3 User settings (Paramètres utilisateur)

Les paramètres utilisateur se trouvent sous **<Settings>** ▸ **<User settings>**.

8.3.1 Set time (Réglage date et heure)

Cette fonction permet de régler la date et l'heure sur l'instrument.

Remarque: L'heure définie ici sera automatiquement modifiée si l'option de synchronisation de l'heure avec le réseau est activée. Pour configurer la synchronisation de l'heure avec le réseau , voir le paragraphe 9.6 « Activation de la synchronisation de l'heure avec le réseau ».

8.3.2 Network Settings (Paramètres réseau)

Ce paramètre contient les informations requises pour l'intégration au réseau. Pour des explications détaillées, se reporter aux paragraphes suivants :

- 9.1 pour l'intégration au réseau
- 9.2 pour la connexion par LDAP
- 9.3 pour le partage des fichiers
- 9.4 pour le transfert des fichiers via FTP
- 9.6 pour la synchronisation de l'heure avec le réseau

Pour configurer la notification par courriel, voir le paragraphe 9.5 « Connexion à un

serveur de courriel ».

8.3.3 Customer settings (Paramètres client)

Les paramètres client sont les paramètres généraux de l'instrument, comprenant la langue, le nom de l'entreprise, le service, la rue, le code postal, la ville, le nom de l'instrument, la personne à contacter et le site.

Le paramètre de notification par courriel figure également dans **< Customer settings >**, voir paragraphe 9.5 « Connexion à un serveur de courriel ».

8.3.4 Module settings (Paramètres du module)

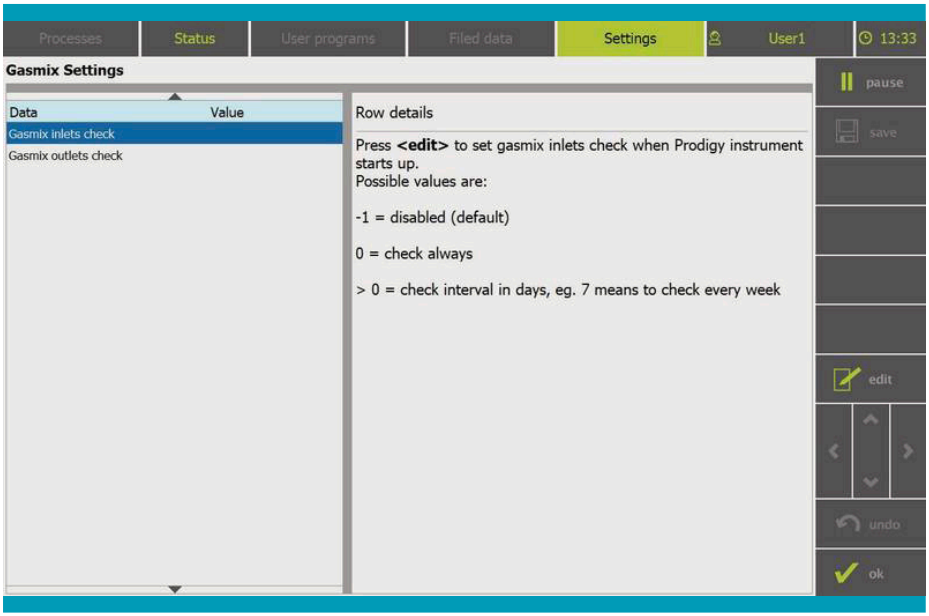
Les paramètres du module contiennent des configurations pour les tests matériels, notamment :

- Contrôle des entrées du mélange gazeux
- Contrôle des sorties du mélange gazeux
- Contrôle de la rotation
- Rappel pour la Supplementary Bag

Pour chacun de ces composants, il est possible de configurer des contrôles à effectuer à différents intervalles de temps :

- Jamais (-1)
- Toujours (0)
- Périodiquement (saisir un nombre de jours).

Pour un exemple de configuration pour les entrées du mélange gazeux (voir Écran 8.10).



Écran 8.10: Contrôle des entrées du mélange gazeux

8.3.5 Settings Exchange (Partage de paramètres)

L'outil **<Settings Exchange>** permet de copier des configurations vers plusieurs instruments. Les paramètres concernés sont les suivants :

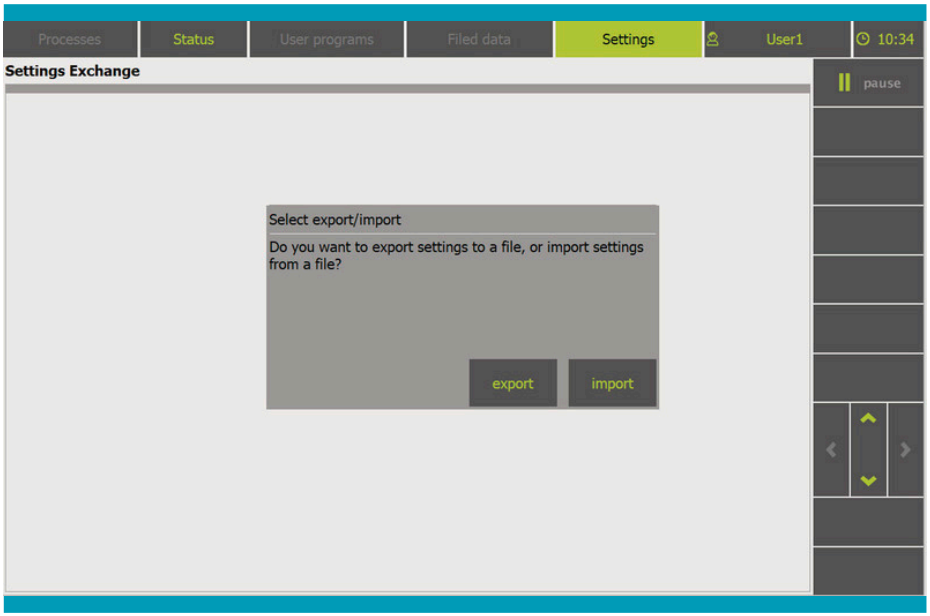
- Customer settings (Paramètres client)
- Gasmix settings (Paramètres du mélange gazeux)
- Module settings (Paramètres du module)
- Network settings (Paramètres réseau)

IMPORTANT

- Si une clé USB est utilisée pour l'importation ou l'exportation, cette clé doit impérativement être de type FAT 32 et ne doit pas être protégée par un mot de passe.
- Si le partage des fichiers est configuré, les fichiers peuvent également être exportés vers le dossier de partage des fichiers (voir paragraphe 9.3 « Connexion à une unité du réseau »).

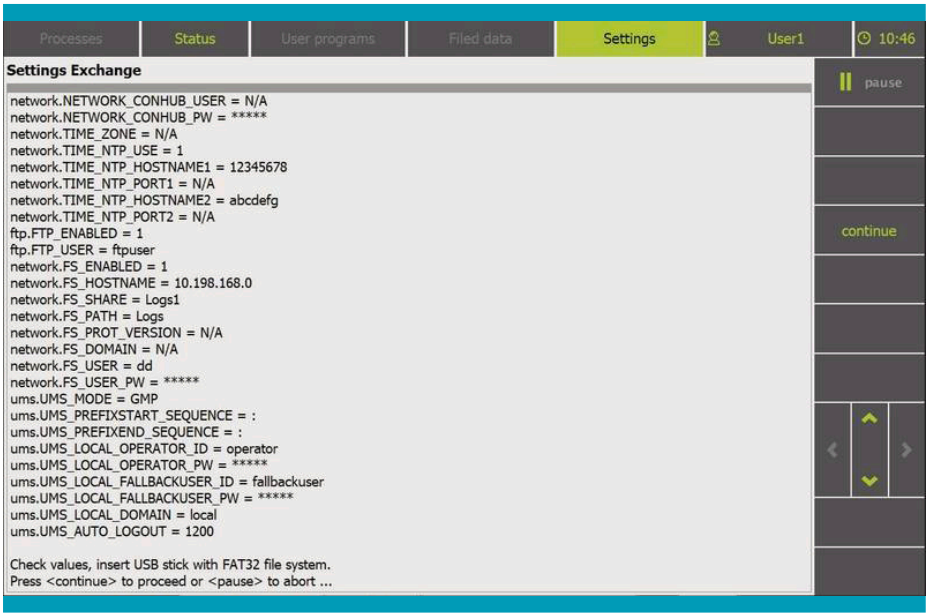
Exportation des paramètres vers une clé USB

1. Insérer une clé USB.
2. Aller dans <Settings> ▸ <User settings> ▸ <Settings Exchange> et appuyer sur <run >.
3. Appuyer sur <export> (exporter) dans la fenêtre contextuelle (voir Écran 8.11).



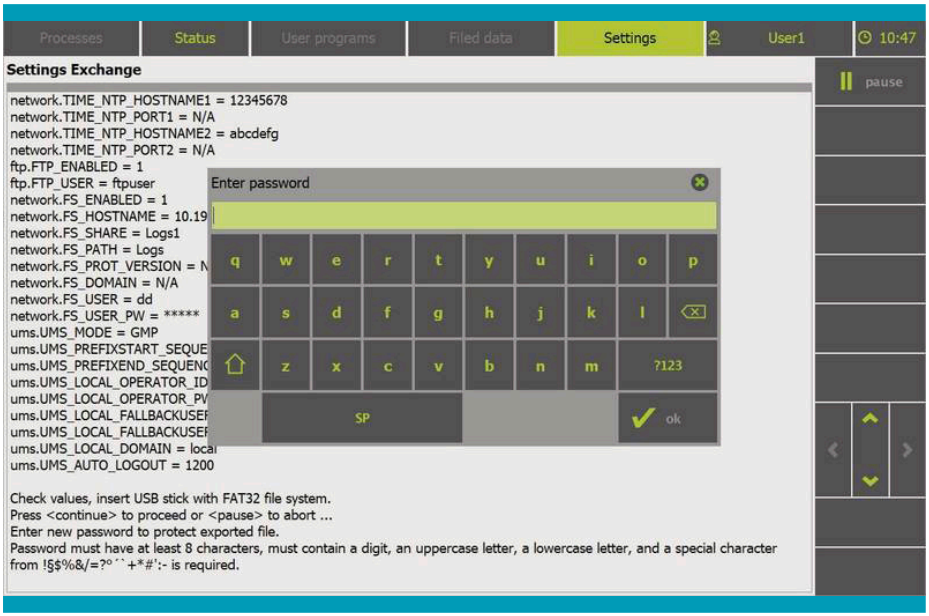
Écran 8.11: Sélectionner export

4. Vérifier les valeurs à l'écran. Appuyer sur <continue> (continuer) dans la barre d'outils.



Écran 8.12: Vérifier les valeurs des paramètres

5. Saisir le mot de passe de connexion.



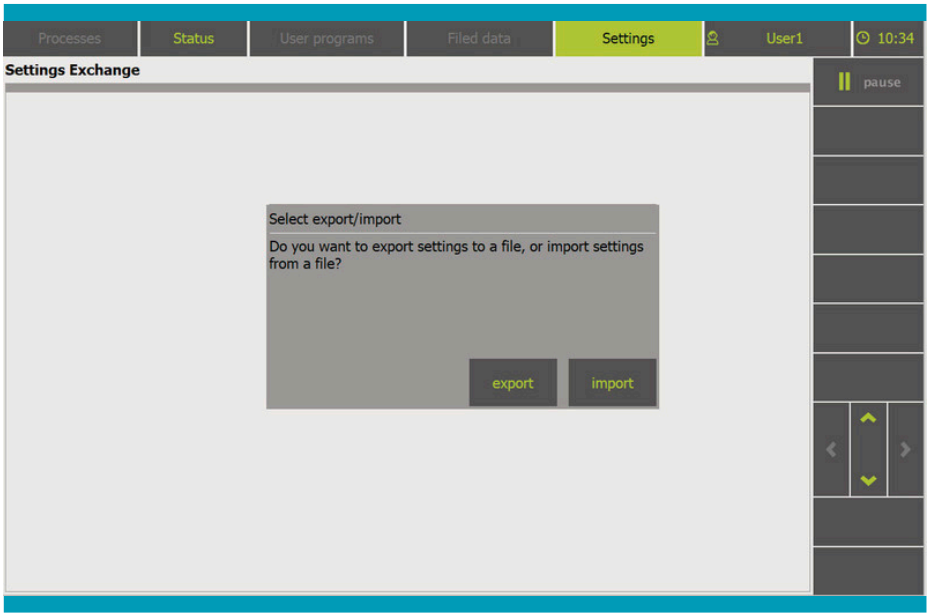
Écran 8.13: Saisir le mot de passe

Importation des paramètres depuis une clé USB

1. Insérer une clé USB contenant le fichier des paramètres utilisateur souhaité.

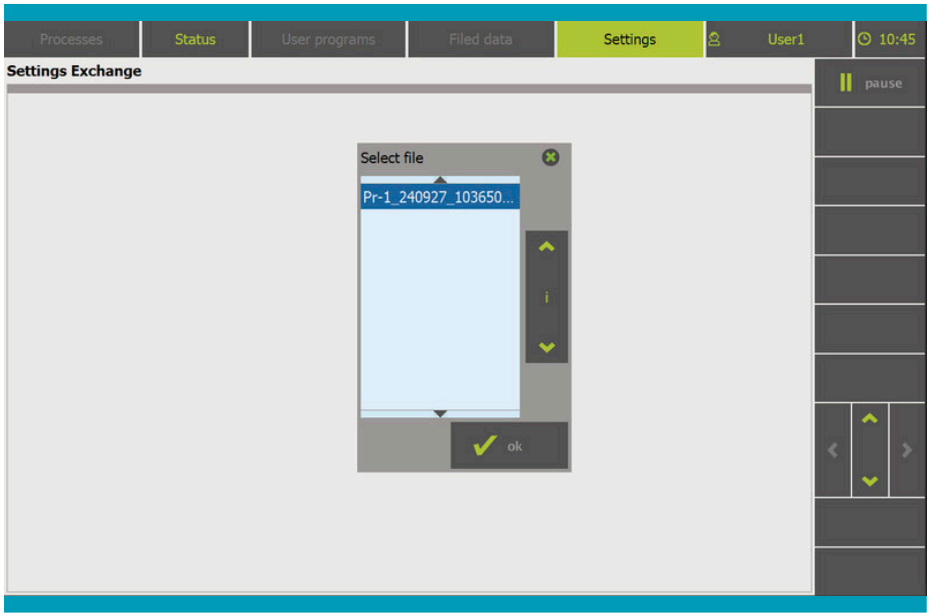
   Remarque: la clé USB doit impérativement être au format FAT 32 et ne doit pas être protégée par un mot de passe.

2. Aller dans <Settings> ▸ <User settings> ▸ <Settings Exchange> et appuyer sur <run >.
3. Sélectionner <Import> (importer) dans la fenêtre contextuelle (voir Écran 8.14).



Écran 8.14: Sélectionner import

4. Sélectionner les fichiers à importer et appuyer sur <ok> (voir Écran 8.15).



Écran 8.15: Sélection du fichier à importer

5. Saisir le mot de passe de connexion (voir Écran 8.13).

8.3.6 SetVolume (Réglage du volume)

Ce programme règle le volume du haut-parleur de l'instrument.

8.3.7 N_2 Settings (Paramètres N_2)

Ce programme configure les deux ports d'entrée de gaz qui seront utilisés parmi les trois disponibles sur l'instrument (N_2, CO_2 air comprimé).

9 Intégration au réseau

L'instrument peut être connecté au réseau local à l'aide d'un adaptateur USB Ethernet. Une intégration au réseau adaptée est requise pour utiliser les fonctions suivantes :

- Gestion centralisée des utilisateurs (LDAP)
- Transfert des fichiers via FTP
- Partage automatique des fichiers
- Notification par courriel
- Synchronisation de l'heure avec le réseau

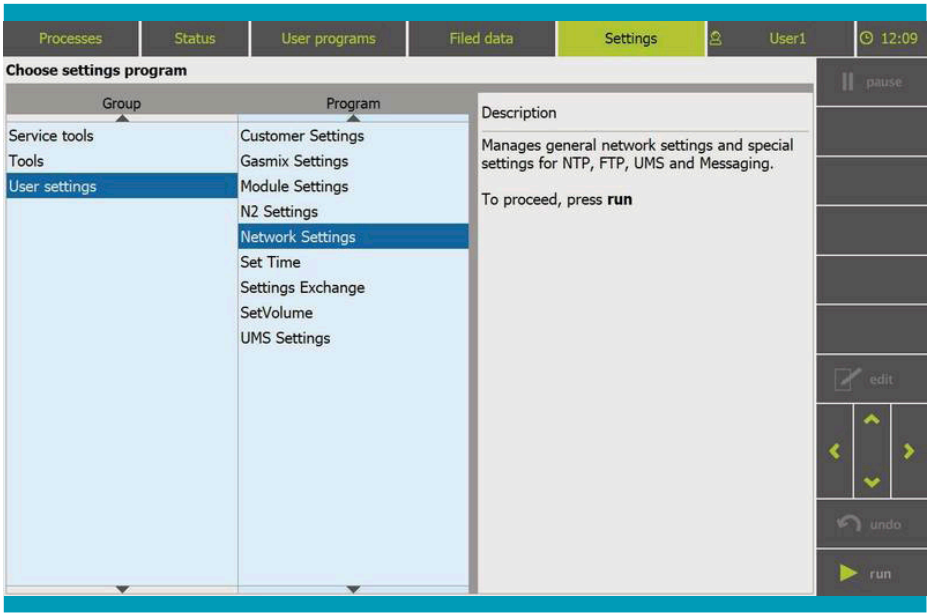
Pour utiliser les fonctions ci-dessus, connecter d'abord l'instrument au réseau local, voir paragraphe 9.1 « Connexion à un réseau local », puis suivre les instructions correspondant aux fonctions spécifiques.

IMPORTANT

- Seuls les utilisateurs UMS ayant le rôle d'administrateur « Administration tools user » ou les utilisateurs disposant des droits « Network Settings » ont accès à ce paramètrage. Pour configurer les droits et les rôles, voir le chapitre 10 « Gestion des utilisateurs ».
- Il est possible que le bouton **<Connectivity Hub>** (Hub de connectivité) soit affiché à l'écran ; toutefois, il est actuellement désactivé et le restera jusqu'à la prise en charge de cette fonction.
- L'utilisateur doit impérativement s'assurer que les paramètres du pare-feu permettent l'échange de données entre l'instrument et le serveur/client souhaité. Le client est responsable de la configuration des paramètres du pare-feu.
- Certaines modifications des paramètres nécessitent de redémarrer l'instrument pour être appliquées.

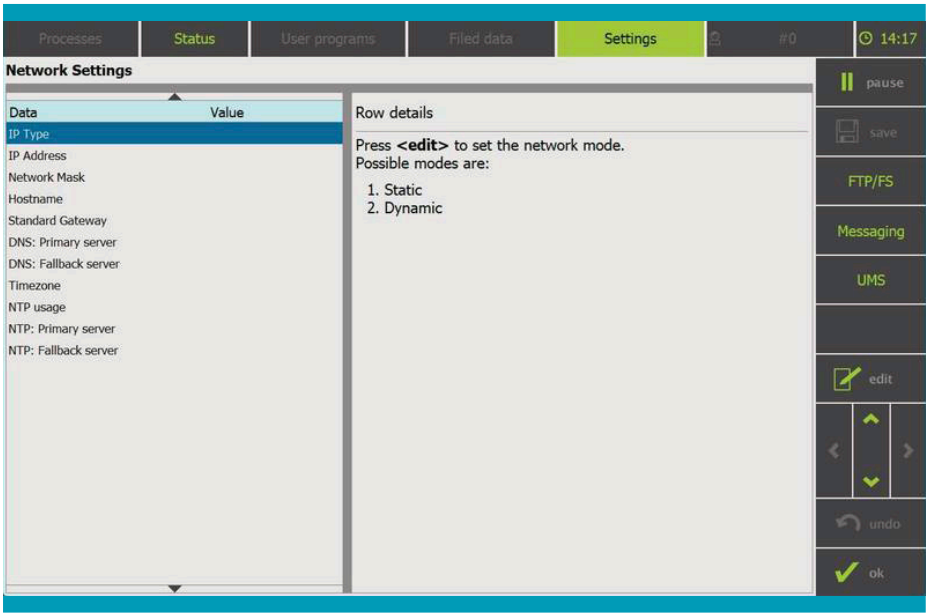
9.1 Connexion à un réseau local

1. Connecter l'instrument au réseau local avec un adaptateur USB Ethernet.
2. Pour saisir les paramètres réseau, aller dans **<Settings>** ▸ **<User settings>** ▸ **<Network Settings>** et appuyer sur **<run>** (voir Écran 9.1). Les paramètres réseau s'affichent (Écran 9.2).



Écran 9.1: Sélectionner Network settings

3. Pour choisir entre adresse IP statique et adresse IP dynamique, sélectionner **<IP Type >** (Type d'IP) dans la liste, puis appuyer sur **< edit>** dans la barre d'outils et saisir la valeur souhaitée dans le champ de saisie.



Écran 9.2: Network Settings (Paramètres réseau

Pour une adresse IP statique, procéder comme suit :

1. Sélectionner < IP Adress > dans la liste, appuyer sur < edit > dans la barre d'outils et saisir l'adresse IP dans le champ de saisie.
2. Sélectionner < Network Mask > dans la liste, appuyer sur < edit > et saisir le masque réseau dans le champ de saisie.
3. Pour saisir le nom de l'instrument, sélectionner <Hostname> (Nom d'hôte) et appuyer sur <edit>.
4. Pour saisir l'adresse IP de la passerelle, sélectionner <Standard Gateway> (Passerelle standard) et appuyer sur <edit>.
5. Facultatif : pour choisir le fuseau horaire, sélectionner < Timezone > et appuyer sur < edit >. Sur l'instrument, le fuseau horaire par défaut est le temps universel coordonné (UTC).
6. Vérifier que l'instrument est connecté au réseau local.

Pour une adresse IP dynamique, procéder comme suit :

1. Pour saisir le nom de l'instrument, sélectionner <Hostname> (Nom d'hôte) et appuyer sur <edit>.
2. Le serveur dynamique doit être configuré. Saisir une adresse IP pour le serveur principal (primary) et le serveur de secours (fallback).
3. Facultatif : pour choisir le fuseau horaire, sélectionner < Timezone > et appuyer

sur < edit >. Sur l'instrument, le fuseau horaire par défaut est le temps universel coordonné (UTC).

4. Vérifier que l'instrument est connecté au réseau local.

IMPORTANT
Si les ports de réseau de votre organisation sont sécurisés par filtrage des adresses MAC, contacter votre prestataire de services informatiques local pour un paramétrage approprié.

9.2 Connexion à un serveur de LDAP

Pour configurer la connexion au serveur LDAP, aller dans (menu d'accès rapide) et sélectionner <User Management>. Dans le menu <User Management>, sélectionner <Configuration> ▸ <LDAP Configuration> (Configuration LDAP). Pour configurer le serveur LDAP, suivre les étapes suivantes (voir Figure 9.1).

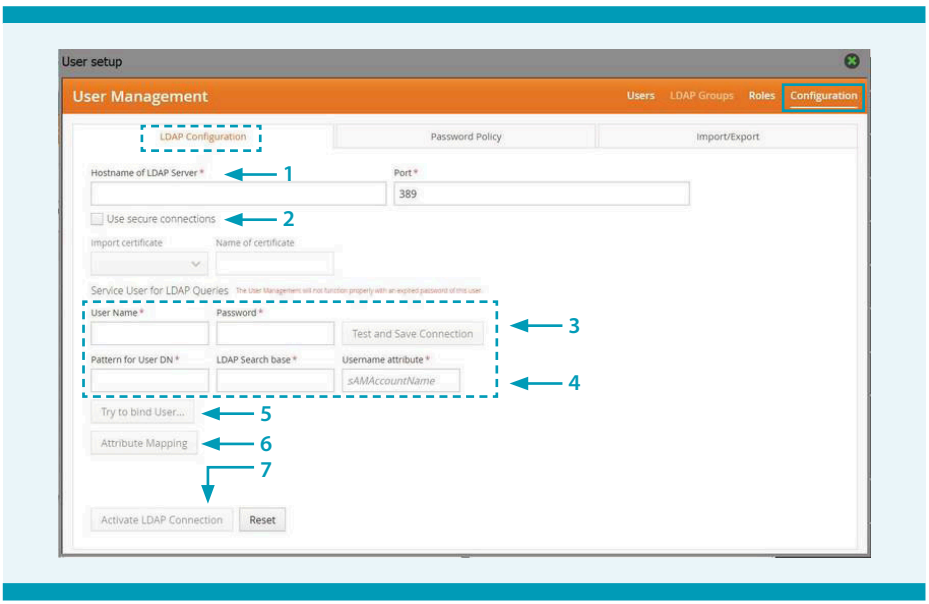


Figure 9.1: Menu User Management et étapes requises pour la configuration du serveur LDAP

1. Saisir le nom d'hôte/l'adresse IP du serveur LDAP.
2. Sélectionner une connexion sécurisée si nécessaire. Le port passe alors automatiquement de la valeur standard 389 au port 636 pour une connexion LDAP sécurisée. Pour une connexion sécurisée, suivre les instructions au paragraphe10.4.2 pour importer le certificat dans l'instrument Prodigy et sélectionner le certificat dans la liste déroulante <import certificate> (importer un certificat).

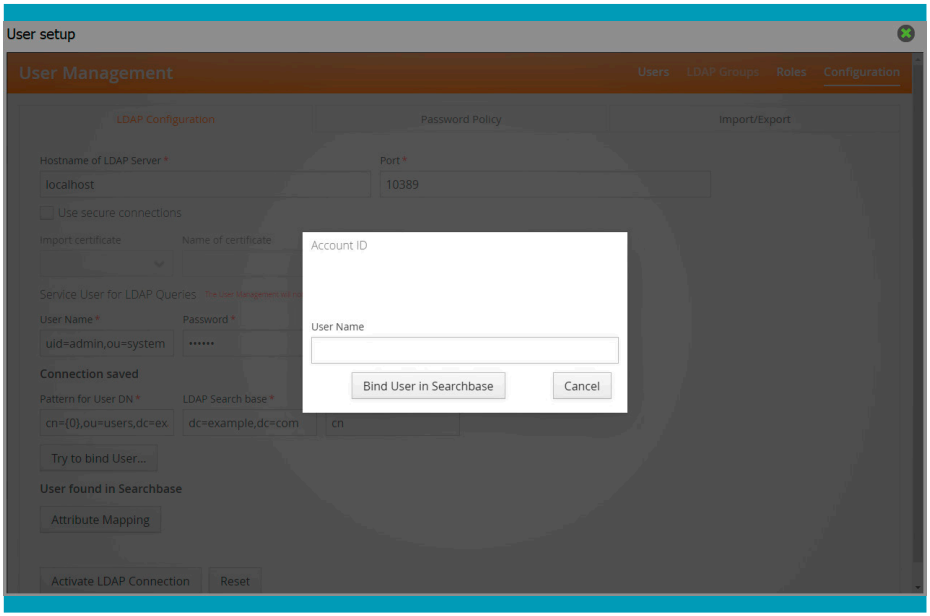
3. Saisir le nom d'utilisateur et le mot de passe d'un compte LDAP valide. Le chemin LDAP complet du nom d'utilisateur doit être saisi. Appuyer sur **<Test and Save Connection>** (Tester et enregistrer la connexion). Une fenêtre contextuelle s'ouvre alors et indique que la connexion a été établie avec succès.

4. Saisir le modèle, la base de recherche et l'attribut du nom d'utilisateur. Le modèle du nom de domaine de l'utilisateur doit contenir le chemin complet. Ces saisies dépendent de la structure organisationnelle du LDAP et du nom de domaine de l'utilisateur. Pour afficher une brève explication et des exemples de valeurs types, survoler les zones de texte. Il peut être utile que quelqu'un ait accès à un programme de navigation LDAP pour afficher les unités organisationnelles qu'il contient.

   Voici des exemples de valeurs types :

   - Modèle = « **<domain>**/{0} », par exemple « customername_dev/{0} » (« nomduclient_dev/{0} »)
   - Base de recherche = « OU=organization,DC=customername » (« OU=organisation,DC= nomduclient »)
   - Attribut de nom d'utilisateur = « sAMAccountName » (« NomduCompte »)

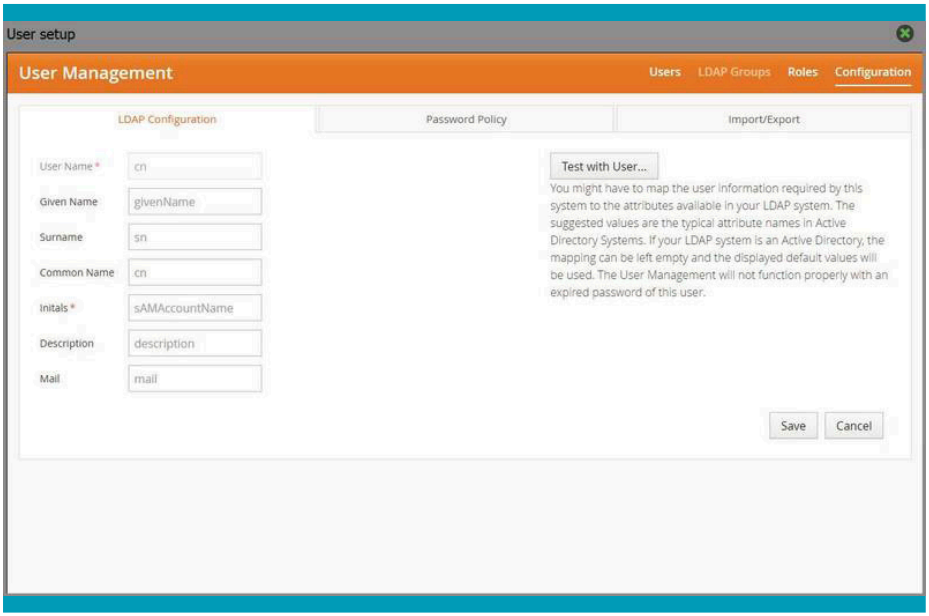
5. Appuyer sur **<Try to bind User…>** (Essayer de lier l'utilisateur...). Une fenêtre contextuelle s'ouvre alors (Écran 9.3). Saisir un nom d'utilisateur valide (le nom d'utilisateur peut être le même que celui utilisé pour l'essai de connexion). Appuyer ensuite sur **<Bind User in Searchbase>** (Lier l'utilisateur dans la base de recherche) pour continuer. En cas de succès, la fenêtre contextuelle Account ID (ID du compte) se ferme ; dans le cas contraire, un message d'erreur s'affiche.



Écran 9.3: Fenêtre contextuelle de saisie Account ID pour la saisie d'un nom d'utilisateur valide

6. Appuyer sur **<Attribute Mapping>** (Mappage des attributs). Le mappage des attributs s'affiche alors (Écran 9.4). L'attribut de nom d'utilisateur saisi à l'étape 4 est automatiquement mis en correspondance avec le nom d'utilisateur. Saisir la même valeur pour « Initials » (« Initiales ») que pour « User Name ». En saisissant des valeurs ici, certaines informations seront consignées automatiquement lors de la création d'un utilisateur. Appuyer sur **<save>** (sauvegarder) pour revenir à la page de configuration du LDAP.

7. Appuyer sur **<Activate LDAP Connection>** (Activer la connexion LDAP). Ce bouton est actif si les étapes 3, 4 et 5 ont été exécutées avec succès.



Écran 9.4: Exemple d'attributs préremplis

IMPORTANT

Il est nécessaire de définir une valeur pour « Initials » (voir Écran 9.4) car cette valeur est considérée comme une information obligatoire pour les utilisateurs du CliniMACS Prodigy. Une configuration manquante ou incorrecte du mappage des attributs peut entraîner un échec de la connexion.

L'exécution de ces sept étapes (voir Figure 9.1) permet de configurer entièrement la connexion LDAP qui peut alors être utilisée pour créer des groupes LDAP et des utilisateurs LDAP dans **<User Management>**. Pour plus de détails sur la gestion des comptes et des rôles, voir le paragraphe 10 « Gestion des utilisateurs ».

9.3 Connexion à une unité du réseau

Le partage automatique des fichiers permet de transférer tous les fichiers journaux vers une unité du réseau après l'exécution d'un processus, immédiatement après la fin de l'application. Les enregistrements sur la piste d'audit peuvent également être exportés vers l'unité de réseau par déclenchement manuel de l'utilisateur (voir paragraphe 7.2.2 « Exportation de la piste d'audit »). Le transfert automatique des fichiers est mis en œuvre sur la base du protocole Server Message Block (SMB). Les versions du protocole SMB prises en charge incluent les versions SMB 1.0, SMB 2.1 et SMB 3.0 (par défaut).

Remarque: Les versions SMB 2.0 et SMB 3.0 sont recommandées. La version SMB 1.0 est uniquement prise en charge pour des raisons historiques et doit uniquement être utilisée pour interagir avec des équipements existants.

Conditions préalables

- Serveur SMB : s'assurer que le serveur SMB est accessible. Vérifier la version du protocole SMB de ce serveur avant de commencer.
- Création préalable d'un dossier sur le serveur SMB pour le stockage des données. Noter le nom de partage. Il peut s'agir d'un partage anonyme (accessible à un compte invité) ou d'un partage authentifié (accessible uniquement au compte spécifié).

  Remarque: Le partage authentifié est recommandé pour la sécurité des données.

- Si un partage authentifié est utilisé, un compte protégé par mot de passe est requis. Ce compte doit avoir un accès en lecture et en écriture au dossier de partage sur le serveur SMB.
- L'instrument est connecté à l'Ethernet et le réseau est activé.

Configuration de l'instrument

Remarque: Il est important de saisir tous les paramètres de partage des fichiers avant d'activer l'option de partage des fichiers car toute modification ultérieure désactive le partage des fichiers. Après la configuration des paramètres, l'instrument doit impérativement être redémarré pour terminer la configuration. Les modifications apportées à la configuration du transfert des fichiers sont appliquées lors du redémarrage.

1. Pour ouvrir les paramètres FTP/partage des fichiers, appuyer sur **<FTP/FS>** dans la barre d'outils (Écran 9.2).
2. Dans **< FTP/File Share Settings>**, seuls les paramètres dans le cadre bleu concernent le partage des fichiers (voir Figure 9.2).

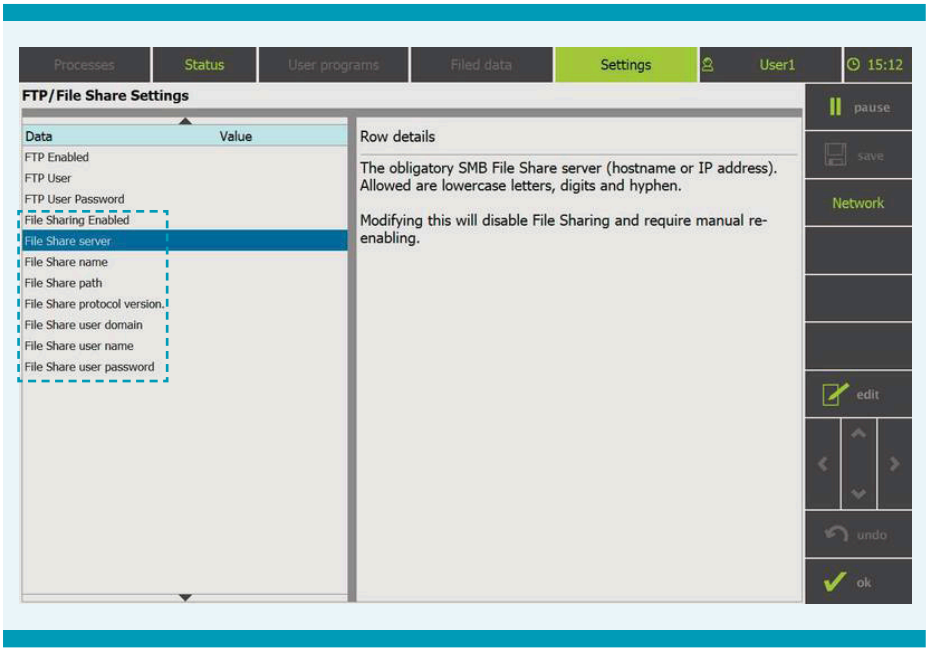


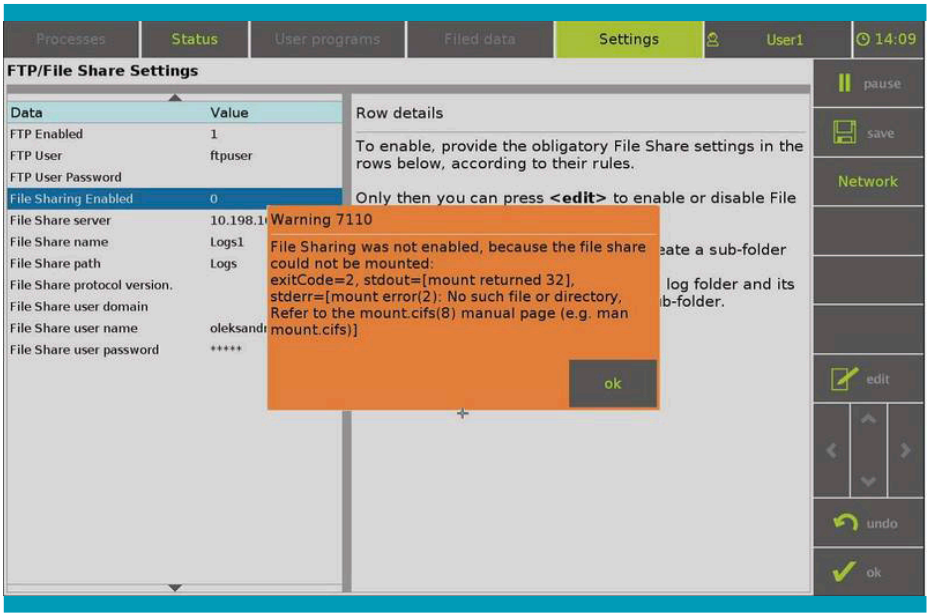
Figure 9.2: Paramètres pour le partage des fichiers

2. Pour saisir le nom d'hôte ou l'adresse IP du serveur SMB, sélectionner **<File Share server>** (Serveur de partage des fichiers) et appuyer sur **<edit>**.
3. Pour saisir le nom de partage, sélectionner **<File Share name>** (Nom de partage des fichiers) et appuyer sur **<edit>**.
4. (Facultatif) Sélectionner **<File Share path>** (Chemin de partage des fichiers) et appuyer sur **<edit>** pour saisir le chemin d'accès.
   Si un chemin d'accès est saisi, les fichiers générés par l'instrument seront transférés vers
   \\[Serveur de partage des fichiers]\[Nom de partage des fichiers]\[Chemin de partage des fichiers]\

   Si aucun chemin d'accès n'est saisi, les fichiers générés par l'instrument seront transférés vers
   \\[Serveur de partage des fichiers]\[Nom de partage des fichiers]\
   Si le dossier est introuvable, le logiciel affiche un avertissement (Écran 9.5).

IMPORTANT

Il est recommandé de ne pas utiliser d'espaces dans le chemin de partage des fichiers.



Écran 9.5: Avertissement concernant un échec de configuration du partage des fichiers

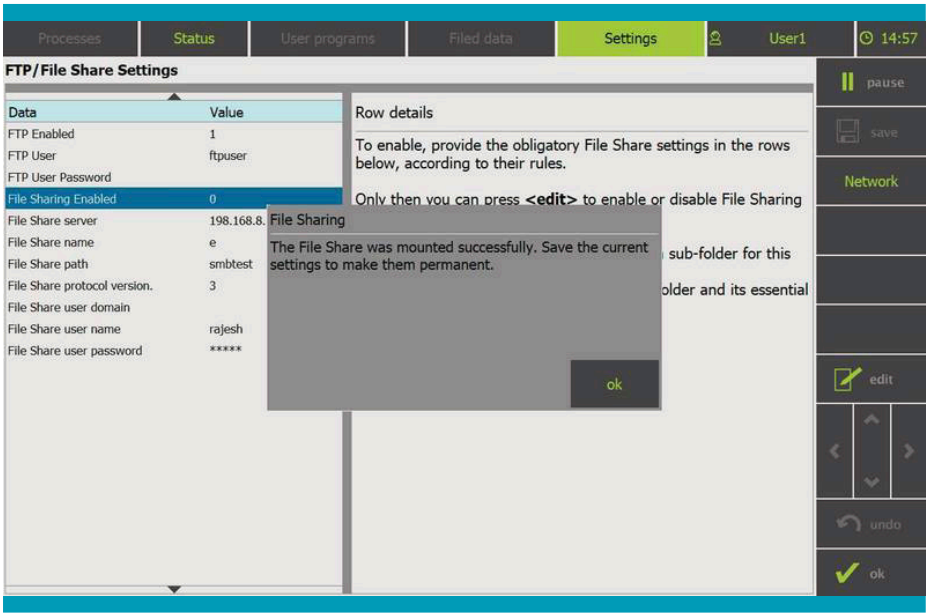
5. Pour saisir la version du protocole SMB, sélectionner **<File Share protocol version>** (Version du protocole de partage des fichiers) et appuyer sur **<edit>**.

6. Pour saisir le domaine de l'utilisateur, sélectionner **<File Share user domain>** (Domaine de l'utilisateur du partage des fichiers) et appuyer sur **<edit>**. Répéter les étapes pour **<File Share user name>** (Nom de l'utilisateur du partage des fichiers) et **<File Share user password>** (Mot de passe de l'utilisateur du partage des fichiers).

IMPORTANT

Si un utilisateur « Guest » (Invité) est utilisé pour partager le dossier de stockage, les champs « File Share user domain », « File Share username « et « File Share user password » doivent impérativement être vides.

7. Définir **<File Sharing Enabled>** (Partage des fichiers activé) sur 1.
   Une fois la configuration terminée, une fenêtre contextuelle indique que la configuration a été effectuée avec succès (voir Écran 9.6).



Écran 9.6: Configuration du partage des fichiers réussie

IMPORTANT

Modifier les paramètres de partage des fichiers a pour effet de désactiver le partage des fichiers qui doit être réactivé manuellement. Toujours vérifier que « File Sharing Enabled » est activé (valeur réglée sur 1).

9.4 Configuration du transfert des fichiers via FTP

FTP est un protocole de réseau qui permet le transfert de données entre le CliniMACS Prodigy (appelé le serveur FTP) et l'ordinateur de l'utilisateur final (appelé le client FTP) par le biais de connexions IP (Internet Protocol).

IMPORTANT

- S'assurer que la connexion FTP est uniquement utilisée sur un réseau interne, sans accès à, ni depuis Internet. La sécurité du réseau doit impérativement être assurée par l'utilisateur.
- S'assurer que les paramètres du pare-feu de l'ordinateur client sont configurés de manière appropriée pour les connexions FTP actives ou passives afin de permettre l'échange de données avec l'instrument.

Remarque: Les données accessibles par FTP à partir du CliniMACS Prodigy sont en lecture seule et peuvent uniquement être téléchargées.

Pour connecter le client FTP à l'instrument, une connexion est requise. L'instrument doit être configuré différemment en fonction de l'option de connexion.

Deux options de connexion sont prises en charge :

- Option de connexion 1 : un compte enregistré dans l'UMS. Vérifier que le rôle « File management user » (Utilisateur des outils de gestion des fichiers) est attribué à ce compte. Dans ce cas, l'établissement et l'interruption de la connexion seront consignés sur la piste d'audit. Pour plus d'informations sur les rôles et sur la gestion des utilisateurs, voir le chapitre 10 « Gestion des utilisateurs ».
- Option de connexion 2 : un nom d'utilisateur local et le mot de passe associé, enregistrés dans FTP/paramètres de partage des fichiers.

9.4.1 Paramétrage de l'instrument

1. Aller dans < FTP/File Share Settings> (FTP/Paramètres de partage des fichiers). Seuls les paramètres dans le cadre bleu concernent le FTP.

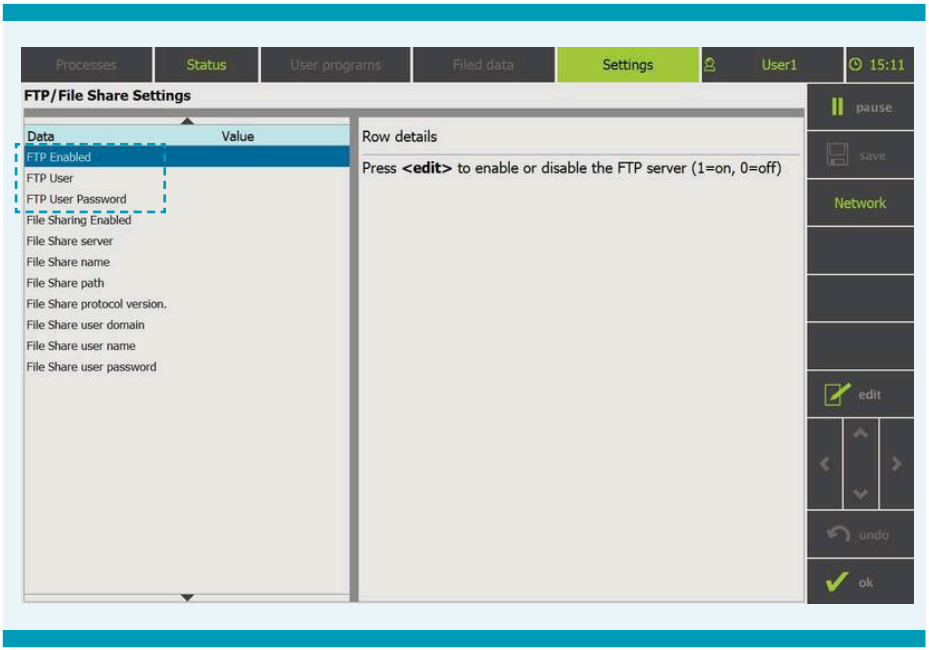


Figure 9.3: Paramètres pour le partage des fichiers

2 (Ignorer cette étape pour l'option de connexion 1) Pour saisir le nom d'utilisateur lors de la connexion à partir du client FTP, aller dans <FTP User> (Utilisateur FTP) et appuyer sur <edit>. Le nom d'utilisateur utilisé pour le client FTP n'a pas besoin d'être enregistré dans le système de gestion des utilisateurs. Le nom d'utilisateur doit impérativement commencer par une lettre et peut se composer de caractères minuscules et majuscules, de chiffres et de tirets bas. **Remarque:** Si <FTP User> est réglé sur « N/A » (« S/O »), la connexion FTP est désactivée.

3. (Ignorer cette étape pour l'option de connexion 1) Pour saisir le mot de passe, aller dans <FTP User Password> (Mot de passe d'utilisateur FTP) et appuyer sur <edit>. Le mot de passe doit impérativement contenir au moins six caractères, dont des caractères minuscules et majuscules, des chiffres et les caractères spéciaux „.:+#!?=.
4. Pour activer la connexion FTP, aller dans <FTP Enabled> et saisir la valeur 1 dans le champ de saisie.
5. Pour enregistrer les paramètres, appuyer sur <ok> dans la barre d'outils.

9.4.2 Connexion au client FTP

L'utilisateur peut se connecter à l'instrument avec n'importe quel client FTP disponible (p. ex. FileZilla) pour télécharger les protocoles et les fichiers journaux après la configuration. Pour se connecter à l'instrument, saisir les informations suivantes :

- Adresse IP de l'instrument. Elle figure dans <Settings> ▸ <Tools> ▸ <Info> ▸ <Network information>.
- Port : utiliser un port 21 standard.
- Nom d'utilisateur et mot de passe :
  pour l'option de connexion 1 : saisir l'identifiant du compte et le mot de passe enregistrés dans la gestion des utilisateurs.
  Pour l'option de connexion 2 : saisir le nom d'utilisateur et le mot de passe configurés, comme décrit précédemment à l'étape 2 et à l'étape 3.

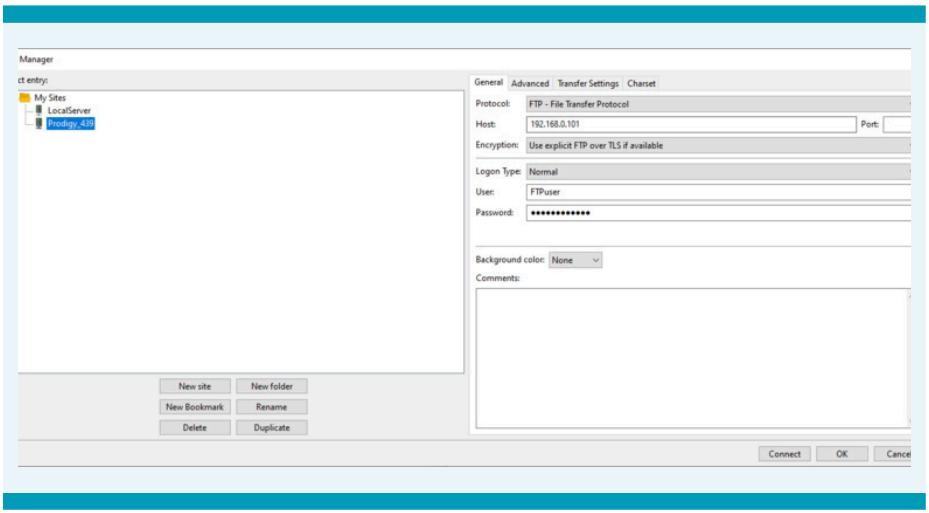


Figure 9.4: Exemple de paramètres de connexion

Remarque: Un utilisateur individuel peut établir une seule connexion à la fois, car les connexions multiples ne sont pas autorisées par le serveur de l'instrument. Si un logiciel client qui utilise des connexions simultanées est utilisé (p ex. FileZilla), modifier les paramètres du client en conséquence pour n'autoriser qu'une seule session. Si cela n'est pas fait, le contenu peut être parcouru mais pas téléchargé.

9.5 Connexion à un serveur de courriel

Le logiciel peut envoyer un courriel à une adresse de courriel prédéfinie en cas de messages d'erreur et/ou d'avertissement pendant l'exécution d'un processus. Le courriel contient les messages d'erreur/d'avertissement et une capture d'écran de l'instrument (voir Figure 9.5). La notification par courriel prend en charge les protocoles Simple Mail Transfer Protocol (SMTP) et Simple Mail Transfer Protocol Secure (SMTPS).

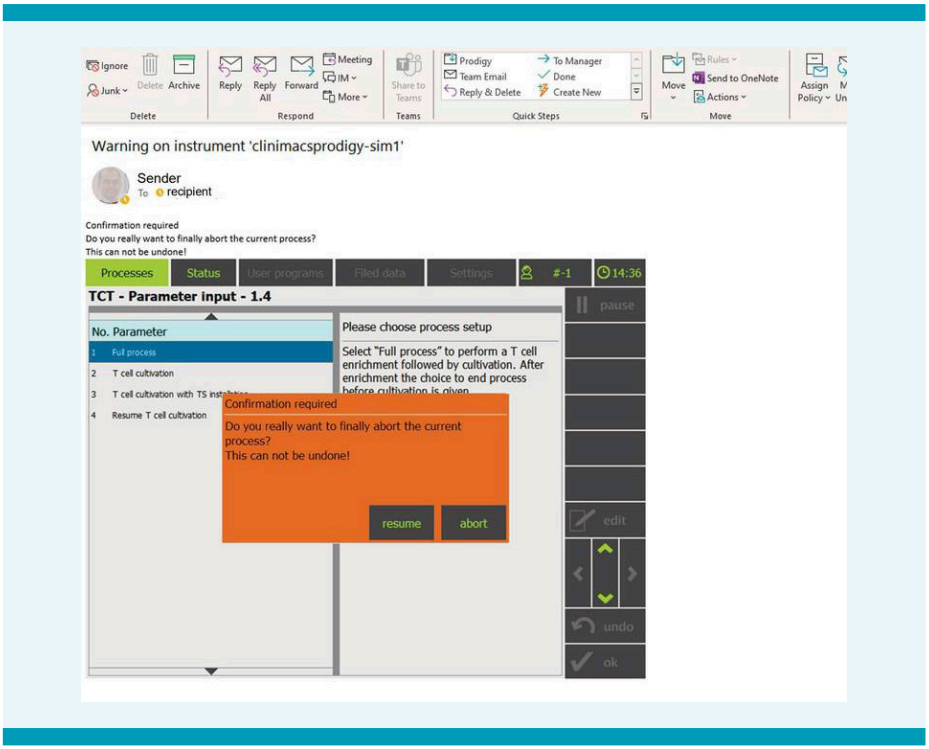


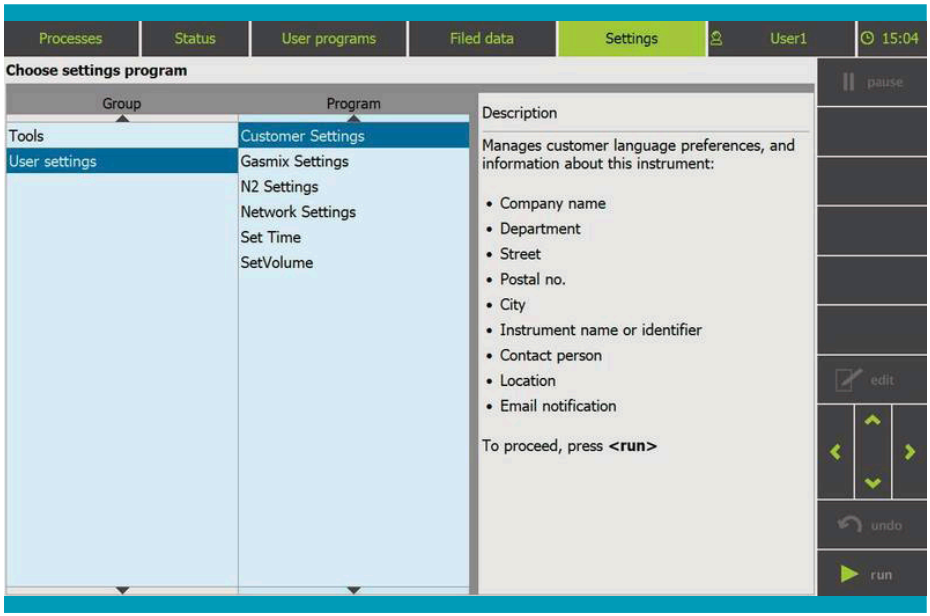
Figure 9.5: Exemple de courriel

Conditions préalables :

- Un serveur de courriel prenant en charge les protocoles SMTP et SMTPS. S'assurer que ce serveur est accessible. Consigner l'adresse IP et le port du serveur.
- Un compte de messagerie électronique créé au préalable par le client et qui peut être utilisé pour l'authentification pendant la configuration.
- L'instrument est connecté à l'Ethernet, et le réseau est activé.

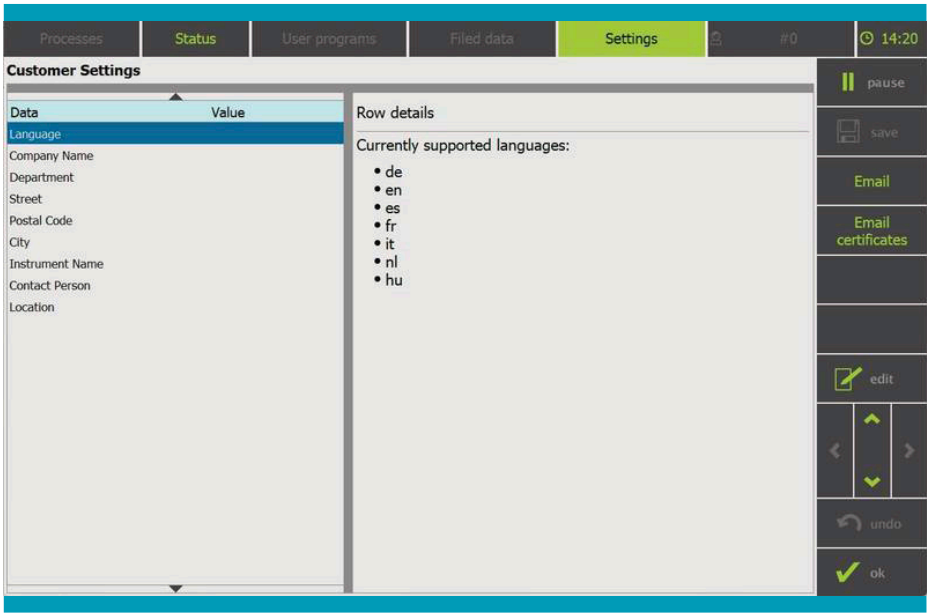
Configuration de l'instrument :

1. Pour saisir les paramètres du client, aller dans <Settings> ▸ <User settings> ▸ <Customer Settings> et appuyer sur <run> (voir Écran 9.7).



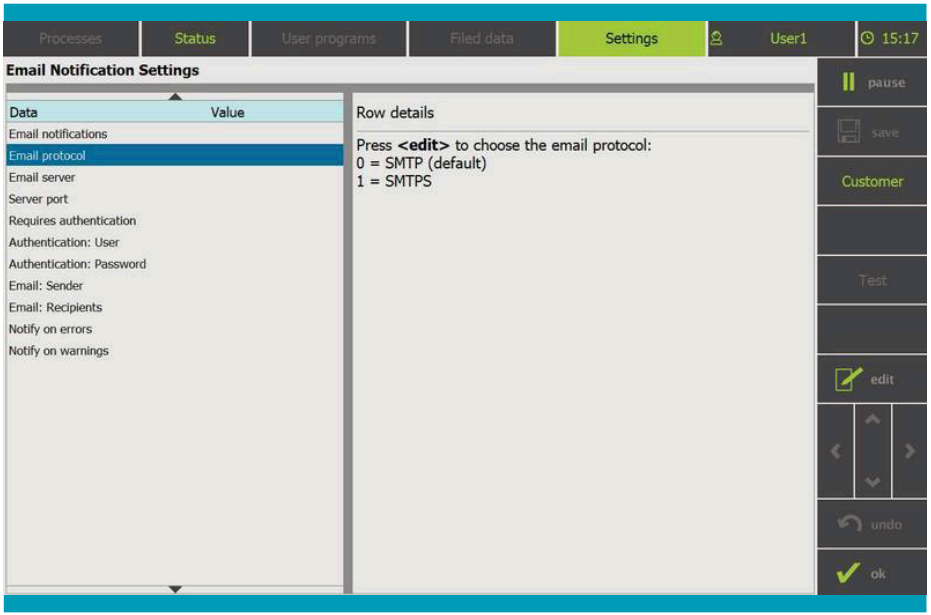
Écran 9.7: Démarrer les paramétrages client

2. Pour entrer dans <Email Notification Settings> (Paramètres de notification par courriel) appuyer sur <Email> (Courriel) dans la barre d'outils (voir Écran 9.8).



Écran 9.8: Paramètres de la messagerie électronique

3. Pour saisir la valeur correspondant au protocole utilisé par le serveur de courriel, aller dans **<Email protocol>** (Protocole de courriel) et appuyer sur **<edit>**. SMTP(0) est sélectionné par défaut.



Écran 9.9: Paramètres de notification par courriel

4. Pour saisir le nom d'hôte ou l'adresse IP du serveur de courriel, aller dans **< Email server>**.

5. Pour saisir le port utilisé dans le serveur de courriel, aller dans **<Server port>** (Port du serveur) et appuyer sur **<edit>**.

Si le port standard est utilisé, il n'est pas nécessaire de modifier ce champ.

Protocole	Port par défaut	Autre port
SMTP	25	2525, 465, 587
SMTPS	465	587 (TLS)

Tableau 9.1: Port pour le serveur de courriel

6. Sélectionner **<Requires authentication>** (Authentification requise). Si le serveur de courriel requiert une authentification, définir la valeur sur 1 dans ce champ et saisir le nom d'utilisateur et le mot de passe d'authentification comme décrit à l'étape 7. Sinon, aller à l'étape 9.

7. Pour saisir le nom d'utilisateur et le mot de passe, aller dans **<Authentication: User >** (Authentification : Utilisateur) et **<Authentication: Password>** (Authentification : Mot de passe).
   Remarque: Plusieurs instruments peuvent partager un compte d'authentification. Consulter votre service informatique pour obtenir de l'aide si nécessaire.

8. Pour saisir l'adresse de courriel de l'expéditeur, aller dans **<Email: Sender>** (Courriel : Expéditeur) et appuyer sur **<edit>**. Le courriel **<Email: Sender>** peut être le même que celui de l'utilisateur d'authentification.

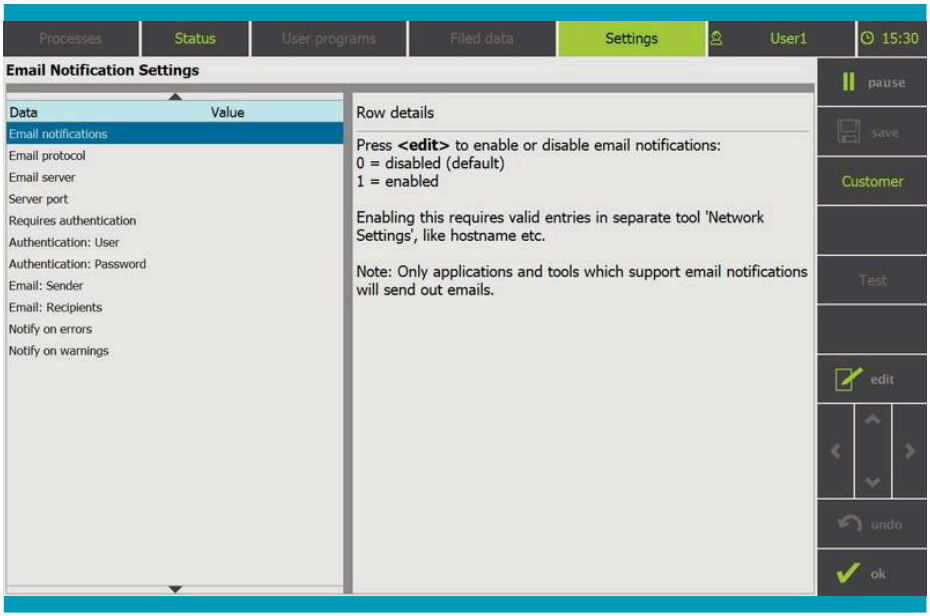
9. Pour saisir les adresses de courriel des destinataires, aller dans **<Email: Recipients >** (Courriel : Destinataires) et appuyer sur **<edit>**. L'adresse des destinataires peut également être une adresse de courriel de groupe.

Remarque: Plusieurs destinataires peuvent être saisis, séparés par un espace.

10. En cas de réception nécessaire des messages d'erreur, aller dans **<Notify on errors>** (Notifier les erreurs) et appuyer sur **<edit>**. Définir sur 1 pour activer les messages. Par défaut, la fonction **< Notify on errors>** est désactivée (valeur définie sur 0).

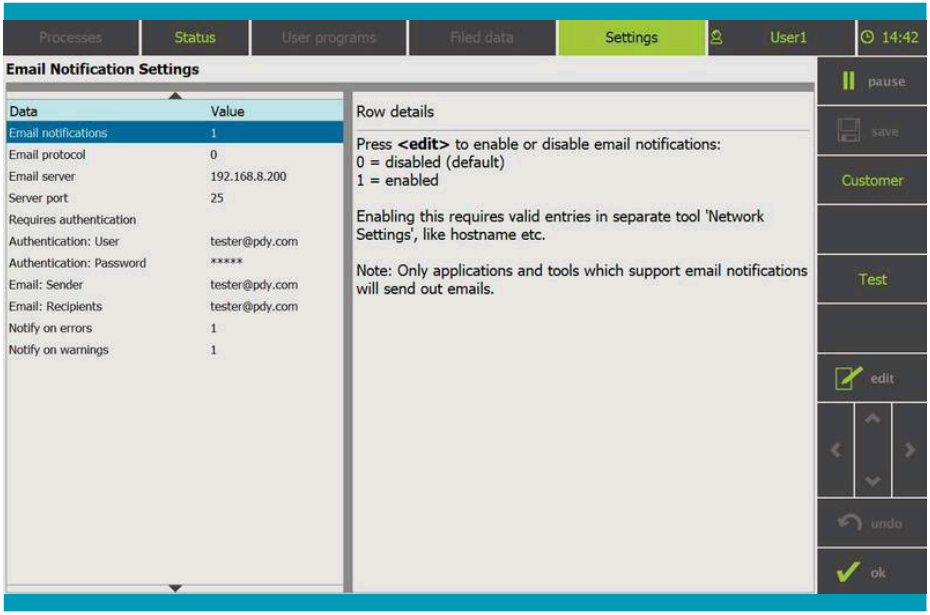
11. En cas de réception nécessaire des messages d'avertissement, aller dans **<Notify on warnings>** (Notifier les avertissements) et appuyer sur **<edit>**. Définir sur 1 pour activer les messages. Par défaut, la fonction **< Notify on warnings >** est désactivée (valeur définie sur 0).

12. Pour activer les notifications par courriel, aller dans **< Email notifications>** (Notifications par courriel) et appuyer sur **<edit>** (voir Écran 9.10). Définir sur 1 pour activer les notifications. Par défaut, les notifications par courriel sont désactivées (valeur définie sur 0).



Écran 9.10: Activer les notifications par courriel

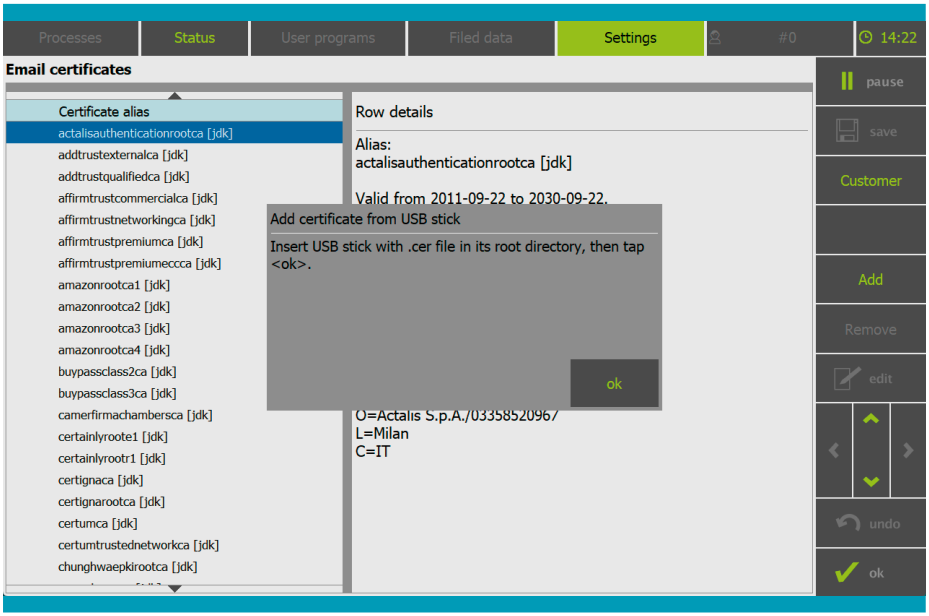
13. Une fois toutes les informations requises saisies, le bouton <Test> est activé dans la barre d'outils. Pour envoyer un courriel de test, appuyer sur <Test> dans la barre d'outils.



Écran 9.11: Envoyer un courriel de test

Certificats de messagerie :

Certains des certificats les plus courants sont disponibles sur l'instrument. Si d'autres certificats sont requis, ceux-ci doivent être ajoutés.



Écran 9.12: Ajouter un certificat à partir d'une clé USB

Pour ajouter un nouveau certificat, appuyer sur < Add > et suivre les instructions à l'écran.

9.6 Activation de la synchronisation de l'heure avec le réseau

Le protocole NTP est un protocole de réseau qui permet la synchronisation de l'horloge et la gestion centralisée de l'heure.

Seuls les utilisateurs UMS ayant le rôle d'administrateur « Administration tools user » ou le rôle « network setting tools user » peuvent accéder aux paramètres réseau. Pour activer la fonctionnalité NTP sur l'instrument, suivre ces étapes :

1. Aller dans <Settings> ▸ <User Settings> ▸ <Network Settings> et appuyer sur <run>. La fenêtre de configuration du réseau apparaît alors. Les paramètres dans le cadre bleu concernent la synchronisation de l'heure avec le réseau (voir Figure 9.6).

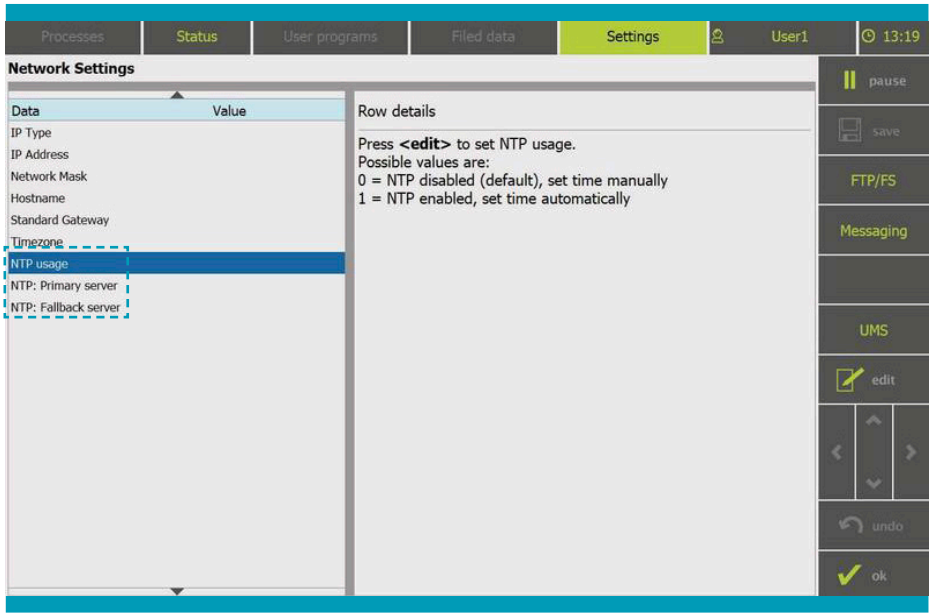


Figure 9.6: Configuration du NTP

2. Pour activer le NTP et régler l'heure automatiquement, appuyer sur <NTP usage> (Utilisation du NTP) et régler la valeur sur 1, puis appuyer sur <ok> dans le champ de saisie.
3. Pour saisir le nom d'hôte/l'adresse IP, appuyer sur <NTP: Primary server> (NTP : Serveur principal) ou <NTP: Fallback server> (NTP : Serveur de secours) puis sur <edit>. Pour confirmer la saisie, appuyer sur <ok>.
4. Appuyer sur <save> et confirmer que ces modifications doivent être acceptées et enregistrées. Les paramètres du serveur NTP sont activés.
5. Redémarrer le système (voir paragraphe 8.7 « Arrêt »).

10
Gestion des utilisateurs

10.1 Informations générales

Le système de gestion des utilisateurs du logiciel prend en charge l'authentification des utilisateurs et le contrôle d'accès basé sur les rôles afin d'assurer la conformité avec la règlementation 21 CFR Part 11.

- Authentification des utilisateurs : un nom d'utilisateur (également appelé identifiant de compte) et un mot de passe sont requis pour se connecter et utiliser l'instrument. La gestion des utilisateurs locaux et l'authentification par LDAP sont toutes deux prises en charge.
- Contrôle d'accès basé sur les rôles : les utilisateurs avec des rôles différents disposent de droits d'accès différents. Trois termes sont définis dans le contrôle d'accès basé sur les rôles : les droits, les rôles et les comptes.

Droits

Les droits représentent l'unité minimale disponible des actions de l'utilisateur. Les droits sont définis par le logiciel et l'utilisateur peut uniquement grouper les droits existants. Pour un aperçu des différents droits dans le logiciel, voir Tableau A.1 dans l'Annexe.

Rôles

Les rôles représentent les fonctions ou responsabilités d'un poste au sein d'une organisation. Un ensemble de droits peuvent être attribués à un rôle. Le logiciel prévoit des rôles par défaut. Les principaux rôles par défaut sont récapitulés dans le Tableau 10.1. Le logiciel prend en charge les rôles personnalisés.

Comptes

Les comptes représentent les utilisateurs individuels. Dans un environnement GMP, il doit y avoir une relation univoque entre un individu et un identifiant de compte. Lors de l'installation, un compte administrateur avec tous les rôles est créé. Ce compte permet à l'utilisateur de créer de nouveaux rôles et de nouveaux comptes selon les besoins.

Rôle	Outils/Droits
Application x.x operator (Opérateur application x.x)	Autorisation d'exécuter cette application dans la version x.x
ATS user (Utilisateur ATS)	Accès au Audit Trail System, y compris affichage, exportation et suppression
Administration tools user (Utilisateur des outils d'administration)	Accès aux outils pour l'administration de l'instrument. Recommandé pour les administrateurs
Common tools user (Utilisateur des outils courants)	Accès aux outils courants : info, licence, arrêt et paramètres utilisateur. Recommandé pour tous les utilisateurs
File management user (Utilisateur des outils de gestion des fichiers)	Accès à l'outil Backup Filed Data et à l'outil Custom Files. Autorise l'accès au fichier journal via FTP
Gas mix tool v1.0 Operator (Opérateur de l'outil de mélange des gaz v1.0)	Accès à l'outil de mélange des gaz
Injected programs (Programmes injectés)	Autorisation d'exécuter des programmes injectés
N_2 settings tools user (Utilisateur des outils de paramétrage de N_2)	Accès à l'outil N_2 settings (Paramètres N_2)
Set time user (Utilisateur avec droit de réglage de l'heure)	Permet de régler l'heure
Support tools user (Utilisateur des outils de support)	Accès aux outils pour l'insertion et le retrait de la chambre, la soudeuse et le contrôle de l'instrument
UM Administrator (Administrateur UM)	Accès à la gestion des utilisateurs « User Management » permettant de gérer les comptes
UM user (Utilisateur UM)	Opérateur défini avec les droits de démarrer et d'exécuter les applications utilisateur

Tableau 10.1: Aperçu des rôles par défaut

Voici un exemple de configuration UMS classique :

- Un administrateur gère les comptes et l'instrument. En général, le rôle d'administrateur permet de configurer et de modifier les comptes, et donne

accès à la gestion des fichiers et aux outils avancés pour les paramètres de l'instrument.

- Un opérateur démarre et exécute des applications sur l'instrument. Le compte opérateur est configuré pour autoriser l'exécution d'un ensemble spécifique d'applications et d'outils sur la base des décisions de gestion des utilisateurs du client en matière d'assistance et de dépannage. Il peut y avoir plusieurs types d'utilisateurs définis par le client, et chaque utilisateur peut se voir attribuer un ou plusieurs rôle(s).

IMPORTANT

Le rôle « UM User » doit impérativement être affecté à un opérateur. Le rôle « UM Administrator » doit impérativement être affecté à un administrateur.

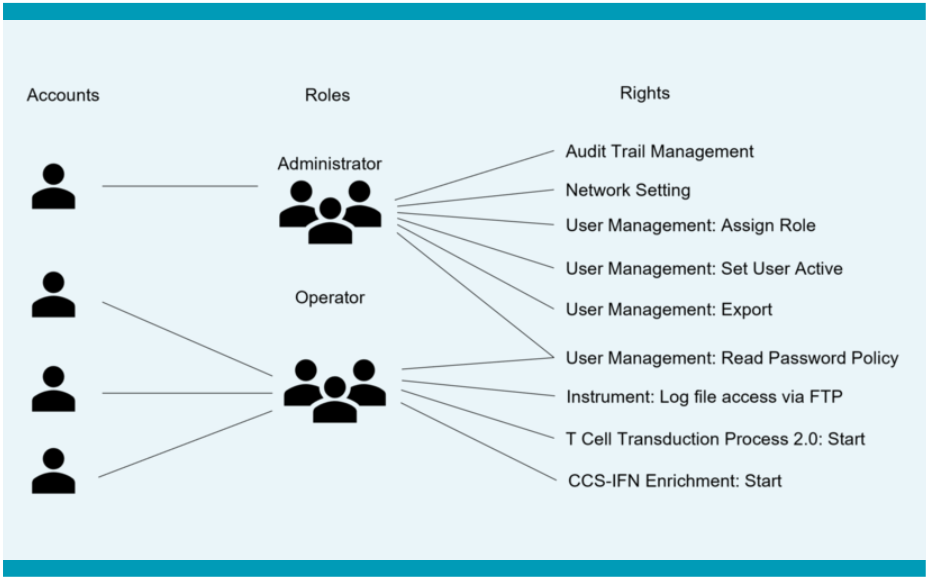


Figure 10.1: Exemple de paramètres de connexion

⚠ ATTENTION

Risque d'échec du processus en raison d'un échec de la connexion. Si la connexion n'est plus possible, il existe un risque d'échec du processus. Pour éviter une telle situation, des comptes utilisateur et administrateur appropriés avec des mots de passe distincts doivent être créés avant de lancer le démarrage d'une application sur l'instrument. Dans le cas où une connexion à l'instrument n'est plus possible, contacter le service Miltenyi Biotec Technical Support.

IMPORTANT

- De plus, il est fortement recommandé de mettre en place une solution « break the glass » pour les situations d'urgence. Il peut s'agir d'un compte

administrateur supplémentaire réservé aux situations d'urgence. Les identifiants de compte pour situation d'urgence doivent être conservés en lieu sûr et n'être accessibles qu'à certaines personnes.

- La procédure d'authentification doit être décrite et mise en œuvre dans le système de gestion de la qualité de l'établissement, et tous les utilisateurs et administrateurs doivent être formés en conséquence.
- En cas d'échec de la connexion par LDAP, utiliser un compte utilisateur local pour accéder à l'instrument.

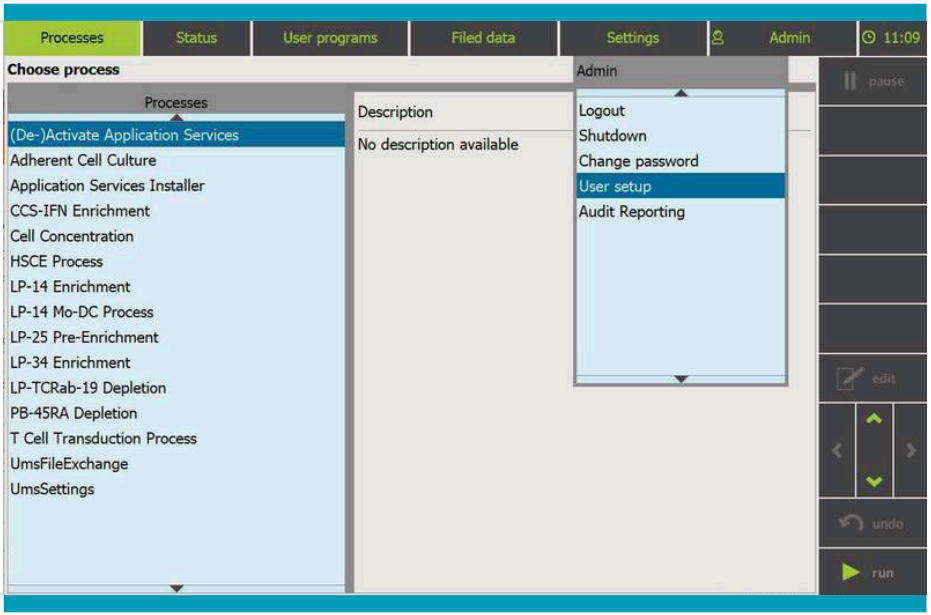
10.2 Gestion des rôles et des comptes

IMPORTANT

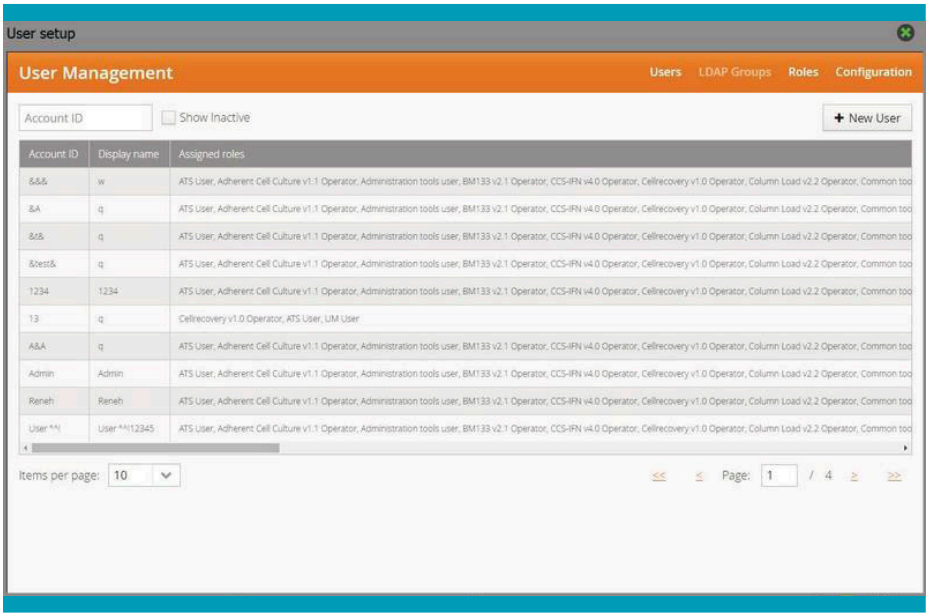
Un utilisateur doit impérativement avoir le rôle « UM Administrator » pour pouvoir configurer le système de gestion des utilisateurs.

10.2.1 Accès à la gestion des utilisateurs

Pour entrer dans le système de gestion des utilisateurs, aller dans (menu d'accès rapide) et appuyer sur **<User setup>**. La page de gestion des utilisateurs s'affiche alors (Écran 10.2). Il existe quatre pages pour la gestion des utilisateurs : **<Users>**, **<LDAP Groups>**, **< Roles>** et **<Configuration>**. Par défaut, la page **<Users>** est sélectionnée.



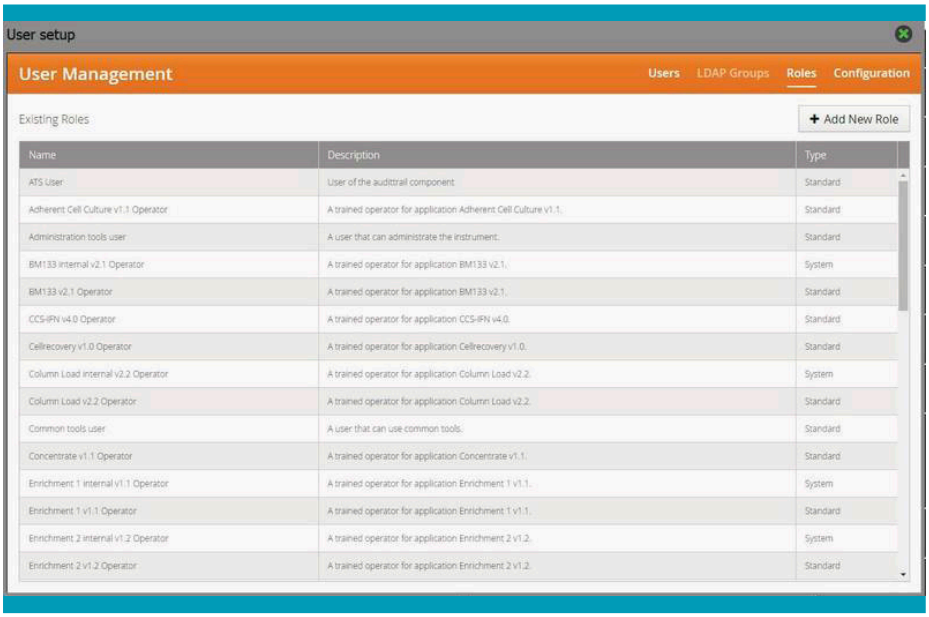
Écran 10.1: Sélectionner User setup



Écran 10.2: Menu User Management

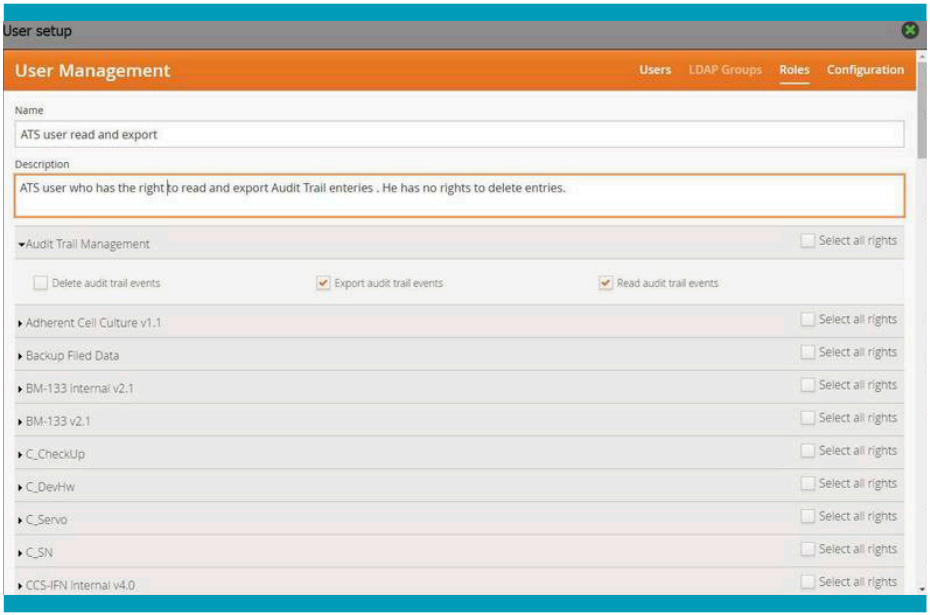
10.2.2 Création d'un nouveau rôle

1. Appuyer sur <Roles> dans <User Management>. Une liste des rôles existants s'affiche alors (Écran 10.3).



Écran 10.3: Rôles définis dans la gestion des utilisateurs

2. Appuyer sur <+Add New Role> (+Ajouter un nouveau rôle, voir Écran 10.3). Une page de définition du nouveau rôle s'affiche alors (voir Écran 10.4).



Écran 10.4: Création d'un nouveau rôle

3. Saisir le nom et la description du rôle. Cocher les droits souhaités pour ce rôle.
4. Appuyer sur <save> au bas de la page. Le nouveau rôle ajouté s'affiche dans la liste des rôles existants et peut être attribué à un utilisateur.

10.2.3 Modification des droits des rôles

1. Trouver et sélectionner le rôle dans la liste des rôles existants (voir Écran 10.3)
2. Sélectionner ou désélectionner les droits souhaités.
3. Faire défiler jusqu'en bas de la page et appuyer sur <save>.

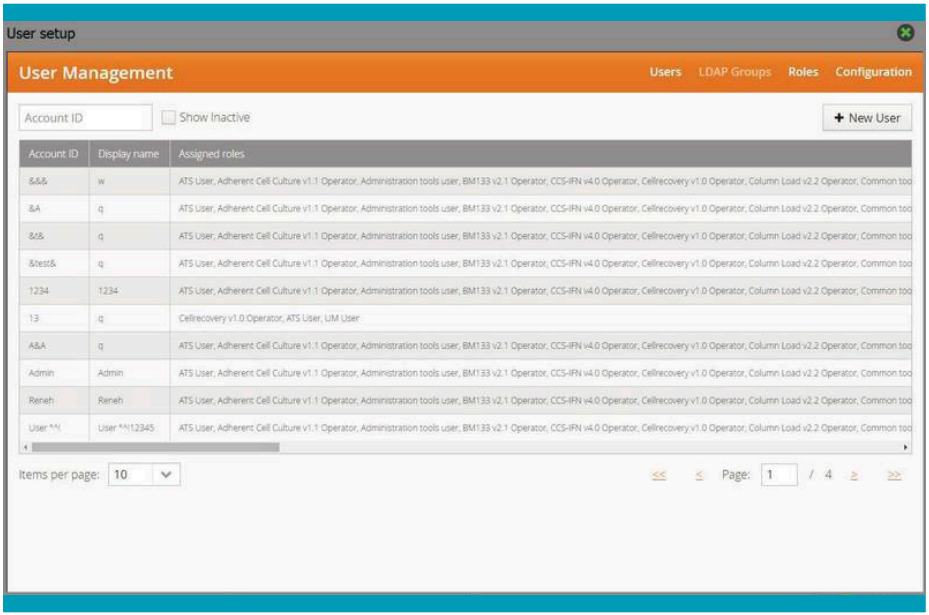
10.2.4 Ajout d'un utilisateur local

IMPORTANT

- Un utilisateur doit impérativement avoir le rôle « UM Administrator » pour créer un nouveau compte.
- Dans un environnement GMP, il faut impérativement utiliser de vrais noms ou synonymes qui peuvent être clairement différenciés et reconnus.

1. Sélectionner le menu <Users> dans la gestion des utilisateurs.

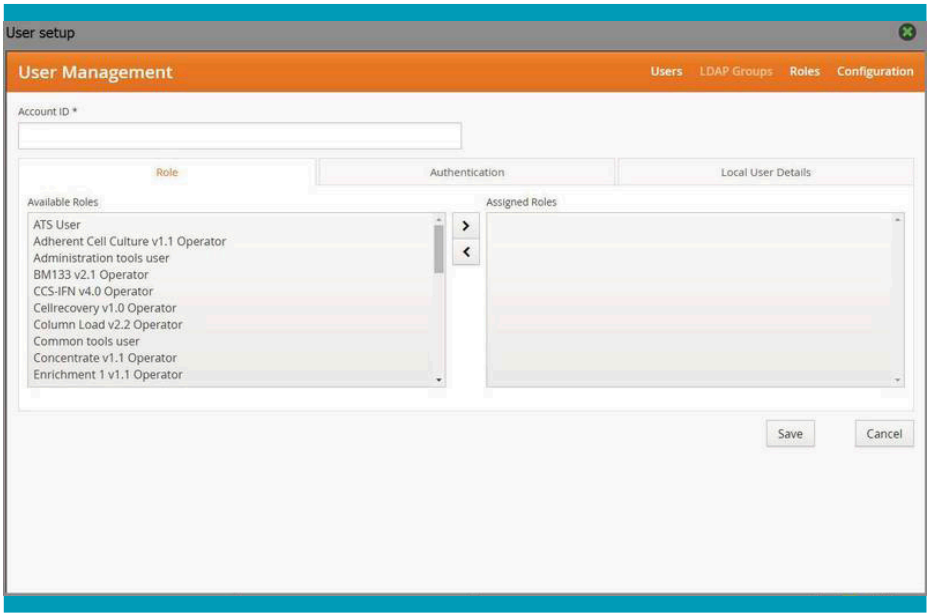
2. Appuyer sur <+New User>. La page de configuration d'un nouvel utilisateur s'affiche alors (Écran 10.5).



Écran 10.5: Menu New User

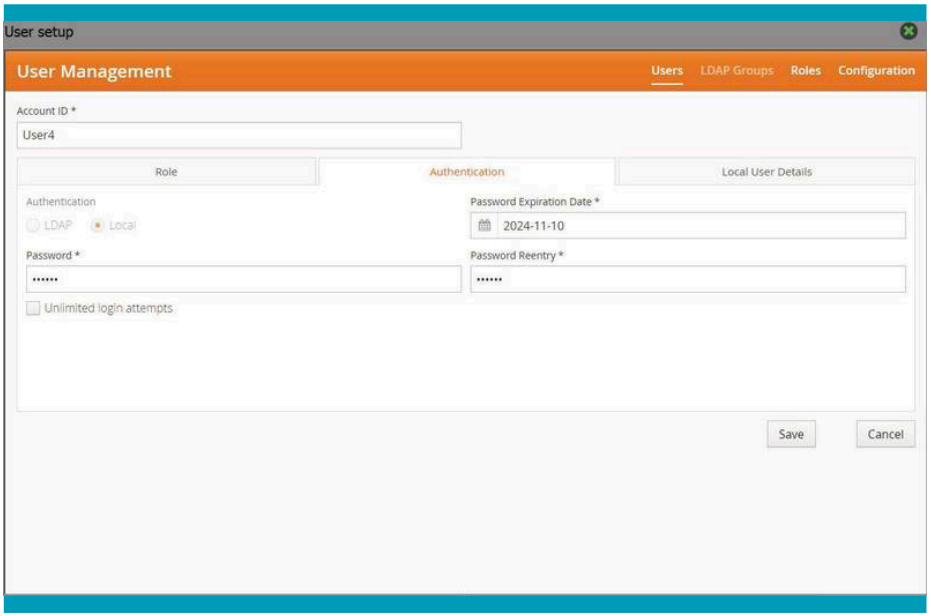
3. Saisir l'identifiant du compte (Écran 10.6). Cet identifiant de compte doit impérativement être unique et avoir une relation univoque avec l'utilisateur final. L'identifiant du compte correspond au nom d'utilisateur utilisé pour la connexion.
   Si Active Directory est configuré, le logiciel vérifiera que cet identifiant est enregistré sur le serveur AD. Si l'identifiant est introuvable, un compte local est créé. Si l'identifiant a été trouvé, le compte AD est utilisé par défaut. Pour transformer un compte LDAP en compte local, suivre l'étape 5.

4. Pour attribuer des rôles à ce compte, sélectionner les entrées correspondantes dans <Available Roles> (Rôles disponibles) dans l'onglet <Role>, et appuyer sur ⊡ (Écran 10.6). Pour supprimer un rôle attribué à ce compte, sélectionner l'entrée correspondante dans <Assigned Roles> (Rôles attribués) et appuyer sur ⊡.



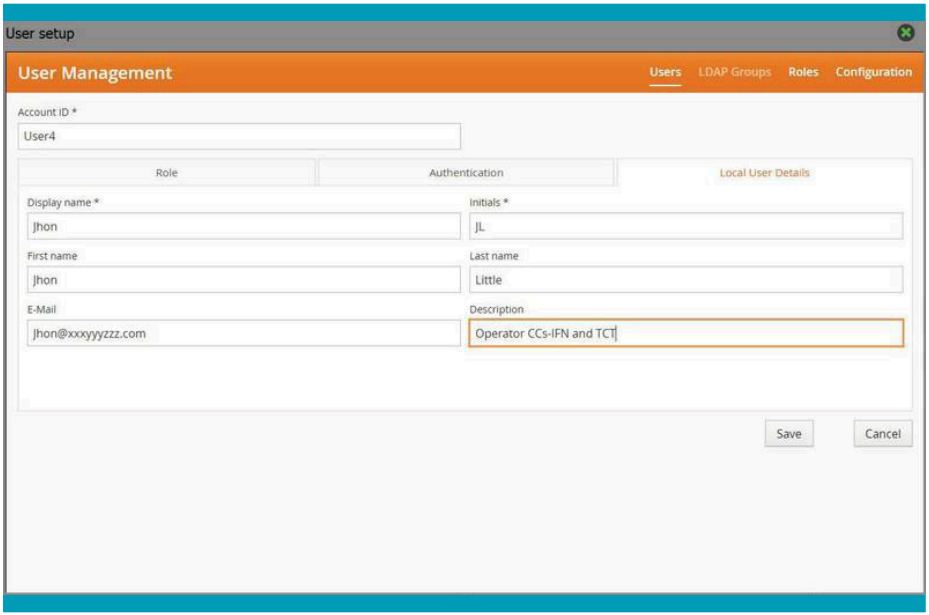
Écran 10.6: Page de configuration de l'utilisateur

5. Si LDAP est configuré et si l'identifiant du compte a été trouvé sur le serveur AD, l'utilisateur peut choisir une authentification via le serveur AD ou via la base de données locale. Pour un utilisateur local, saisir le mot de passe et définir la date d'expiration en suivant la politique en matière de mots de passe (voir paragraphe 10.3 « Configurer la politique en matière de mots de passe »).



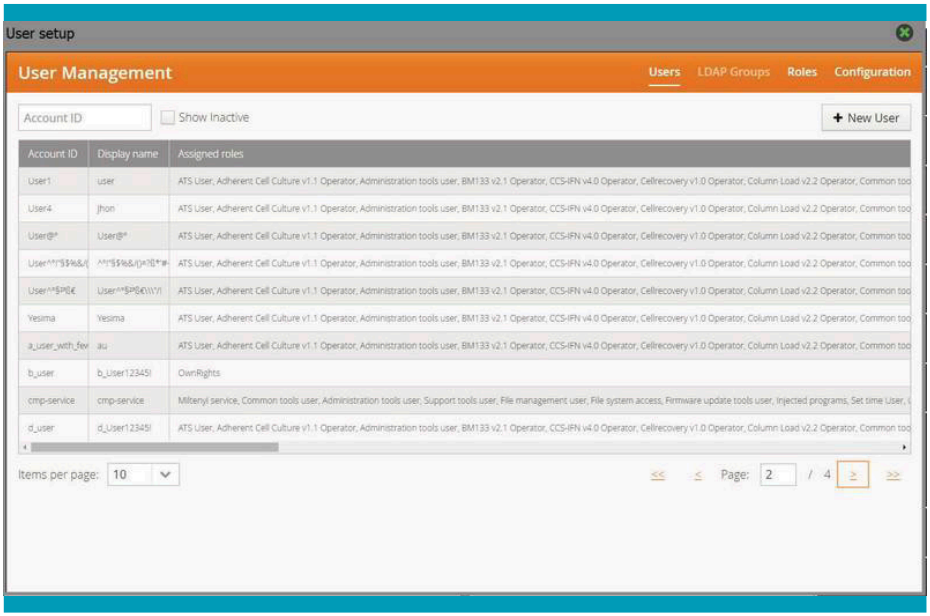
Écran 10.7: Saisie du mot de passe du nouvel utilisateur

6. Dans l'onglet <Local User Details> (Détails sur l'utilisateur local), saisir des informations plus détaillées sur ce compte.



Écran 10.8: Saisie des détails relatifs à l'utilisateur local

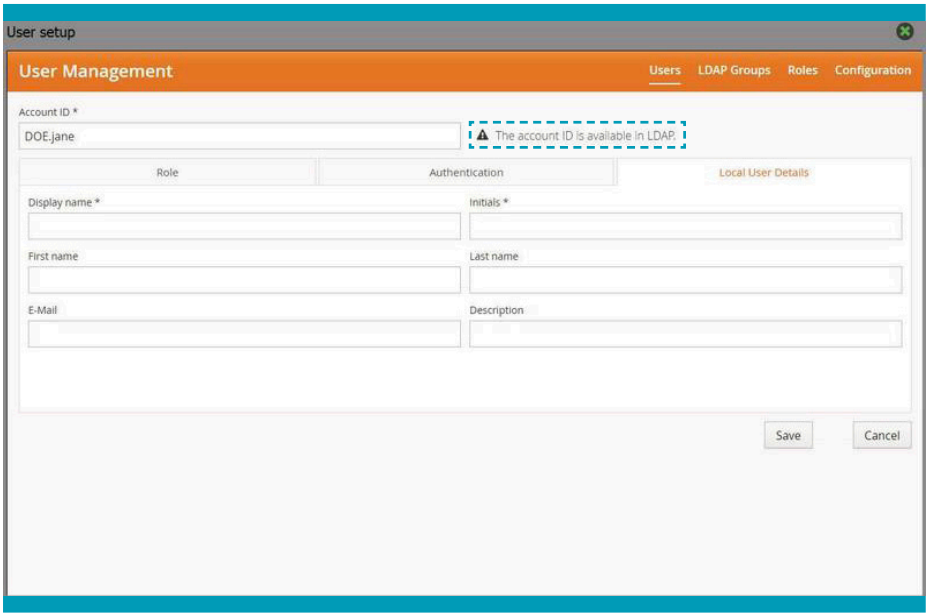
7. Appuyer sur <save>. Le compte nouvellement ajouté s'affiche dans la liste des comptes (Écran 10.9).



Écran 10.9: Confirmation de l'ajout du nouvel utilisateur

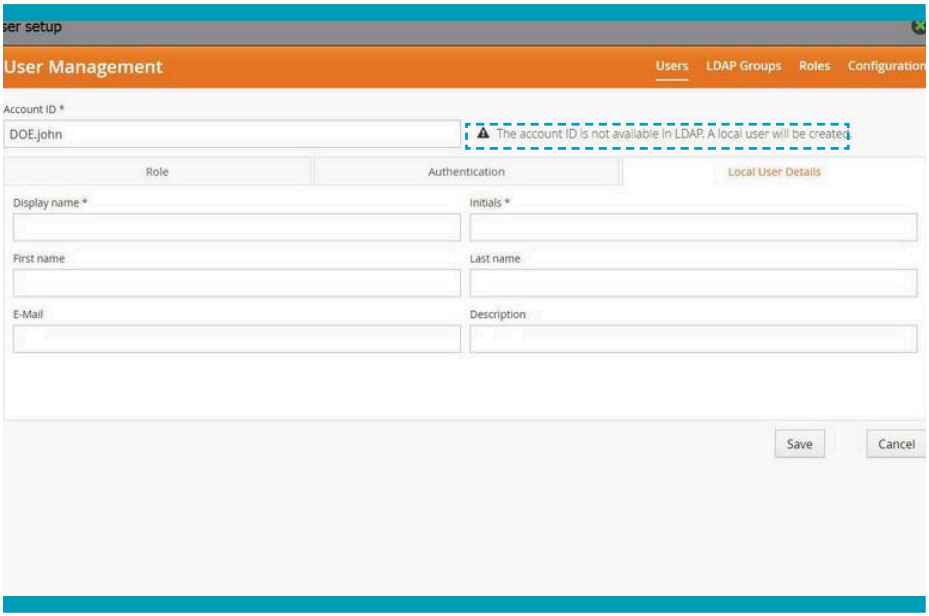
10.2.5 Ajout d'utilisateurs LDAP

1. Aller dans <Users> dans <User Management>.
2. Appuyer sur <+New User>.
3. Saisir l'identifiant du compte LDAP. Le logiciel vérifiera si cet identifiant est enregistré sur le serveur AD. Si l'utilisateur existe déjà, des informations supplémentaires sont insérées à l'aide du mappage des attributs (voir Écran 10.10). Si l'utilisateur n'est pas enregistré dans AD, un nouvel utilisateur local sera créé (voir Écran 10.11).



Écran 10.10: Menu LDAP Users dans User Management montrant un exemple d'utilisateur enregistré

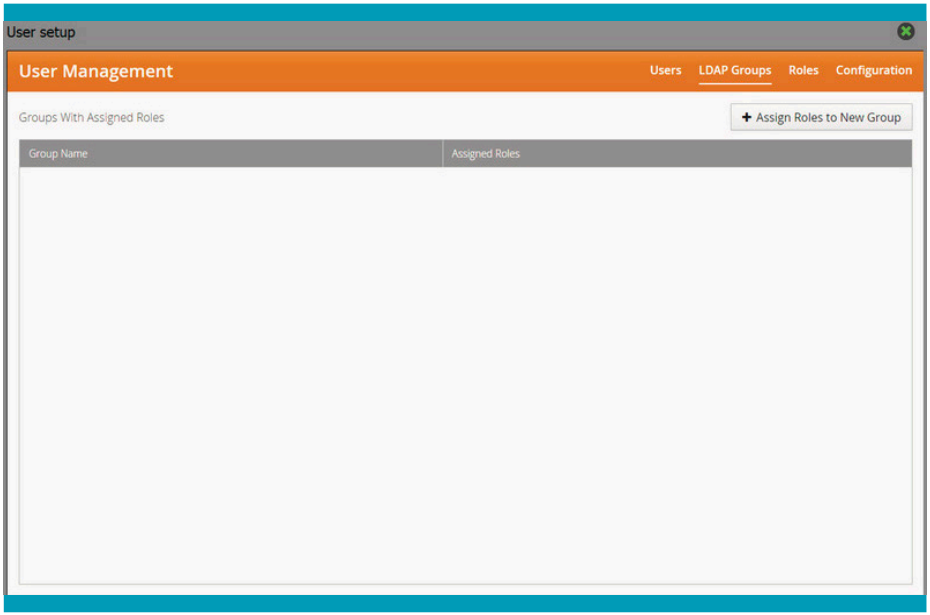
4. Pour attribuer des rôles, appuyer sur <Role> et sélectionner le rôle souhaité.
5. Appuyer sur <save>. L'utilisateur peut utiliser l'identifiant et le mot de passe du compte LDAP pour se connecter.



Écran 10.11: Menu LDAP Users dans User Management montrant un exemple d'utilisateur non enregistré

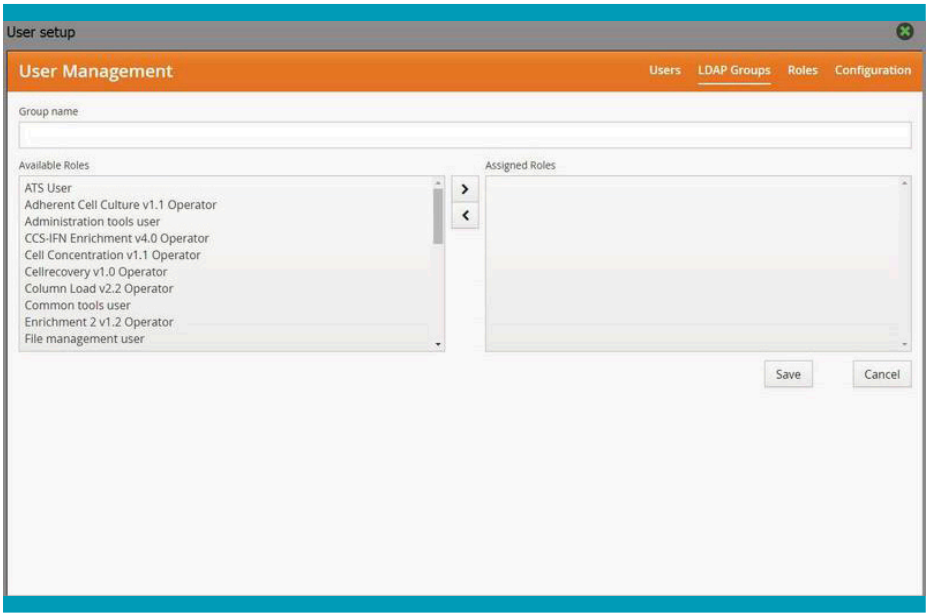
10.2.6 Ajout de groupes LDAP

1. Sélectionner <LDAP Groups> (Groupes LDAP) dans la barre de menu et appuyer sur <+ Assign Roles to New Group> (Attribuer des rôles à un nouveau groupe).



Écran 10.12: Menu User Management et étapes requises pour l'ajout de groupes LDAP

2. Saisir le nom du groupe (voir Écran 10.13). Le système vérifie automatiquement si ce groupe existe dans LDAP.
3. Pour attribuer des rôles à ce groupe, sélectionner les rôles dans <Available Roles> et appuyer sur ⊡. Pour supprimer un rôle attribué à ce groupe, sélectionner l'entrée correspondante dans <Assigned Roles> et appuyer sur ⊡.
4. Appuyer sur <save>.



Écran 10.13: Menu LDAP user groups dans User Management

IMPORTANT

S'assurer d'ajouter le bon « UM Administrator » ou « UM User » afin de garantir une connexion correcte.

10.2.7 Modification des rôles attribués à un utilisateur ou à un groupe LDAP

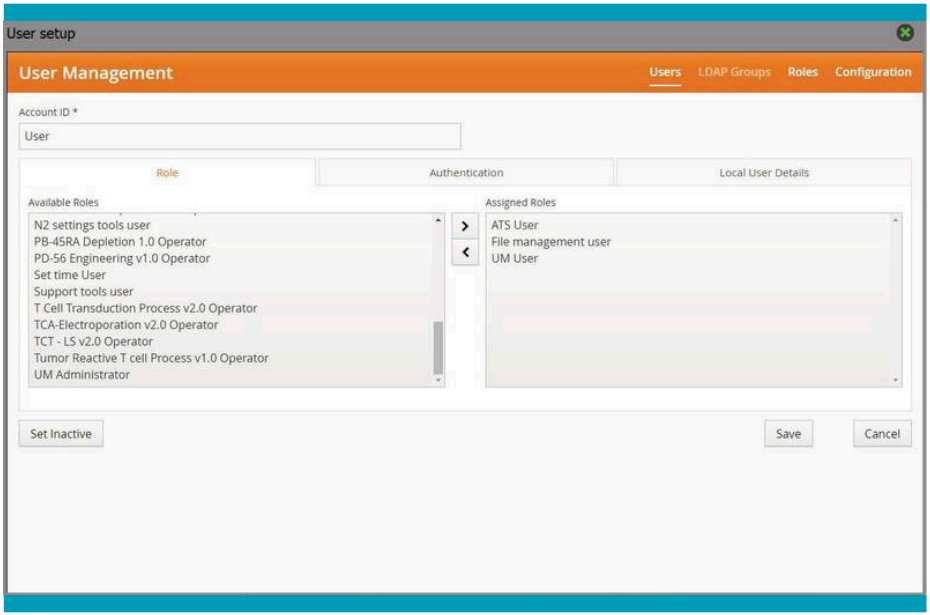
1. Sélectionner l'utilisateur dans la liste des utilisateurs dans la page « Users » (Écran 10.2) et appuyer sur l'élément. Pour un groupe LDAP, sélectionner le groupe souhaité sur la page LDAP Groups (Écran 10.12).
2. Pour attribuer des rôles supplémentaires à l'utilisateur, sélectionner les entrées correspondantes dans **<Available Roles>** dans l'onglet **<Role>** et appuyer sur ›. Pour supprimer des rôles attribués à ce compte, sélectionner les entrées correspondantes dans **<Assigned Roles>** et appuyer sur ‹.
3. Appuyer sur **<Save>** en bas de l'onglet **<Role>**.

10.2.8 Désactivation d'utilisateurs locaux

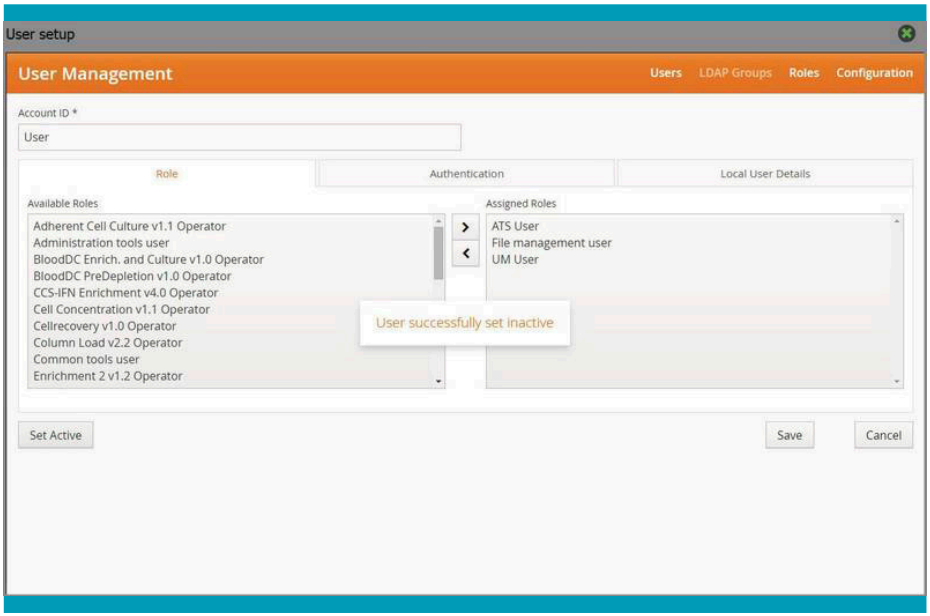
Remarque : Un utilisateur local ne peut pas être supprimé, il peut uniquement être désactivé.

1. Sélectionner un utilisateur local dans la liste des utilisateurs (Écran 10.9). La page de configuration des utilisateurs s'ouvre alors.

2. Appuyer sur <Set Inactive> (Rendre inactif) en bas de la page de configuration des utilisateurs (Écran 10.14).

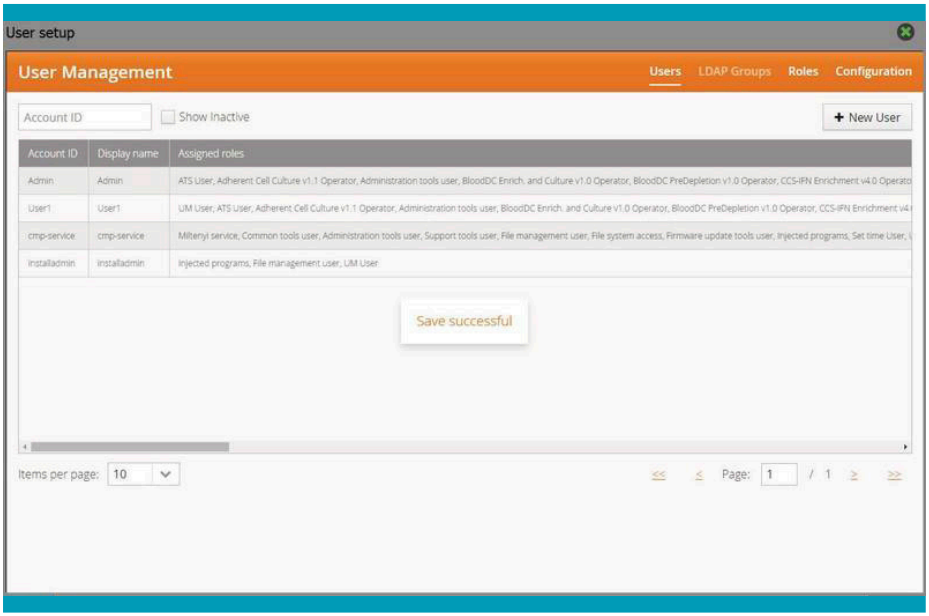


Écran 10.14: Désactivation d'un utilisateur local



Écran 10.15: Utilisateur désactivé avec succès

3. Appuyer sur <Save> en bas pour revenir à la liste des utilisateurs.

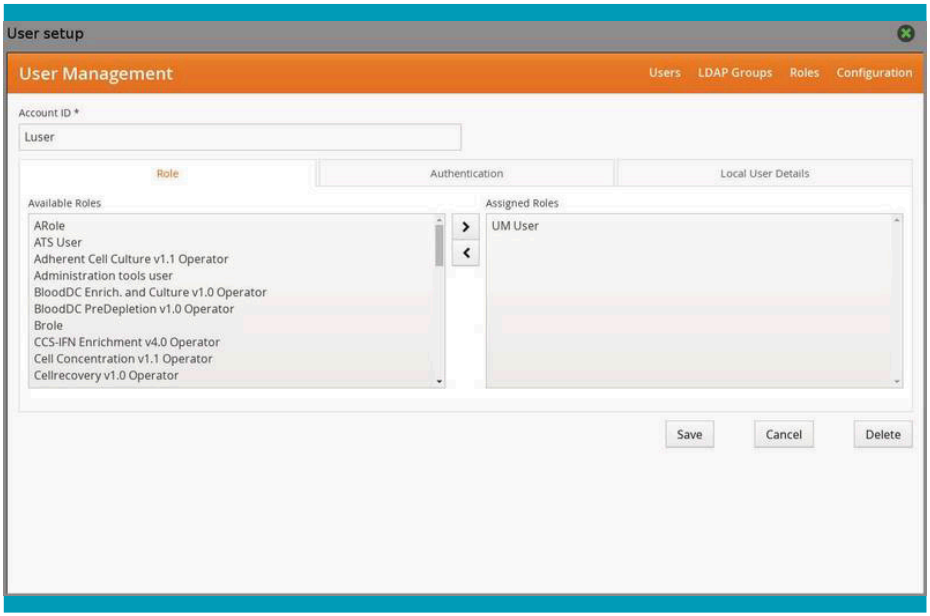


Écran 10.16: Enregistrement réussi

Le compte désactivé n'est pas affiché dans la liste des utilisateurs. Néanmoins, le compte reste enregistré sur l'instrument. Pour voir ou réactiver ce compte, cocher **<Show Inactive>** (Afficher les inactifs, voir Écran 10.16) et suivre la même procédure qu'au paragraphe 10.2.7 « Modification des rôles attribués à un utilisateur ou à un groupe LDAP ».

10.2.9 Suppression d'utilisateurs LDAP

1. Sélectionner un utilisateur LDAP ou un groupe LDAP dans la liste des utilisateurs.
2. Dans la page de configuration des utilisateurs, appuyer sur **<Delete>** (voir Écran 10.17).



Écran 10.17: Suppression d'un utilisateur LDAP

3. Appuyer sur <Save> en bas pour revenir à la liste des utilisateurs.

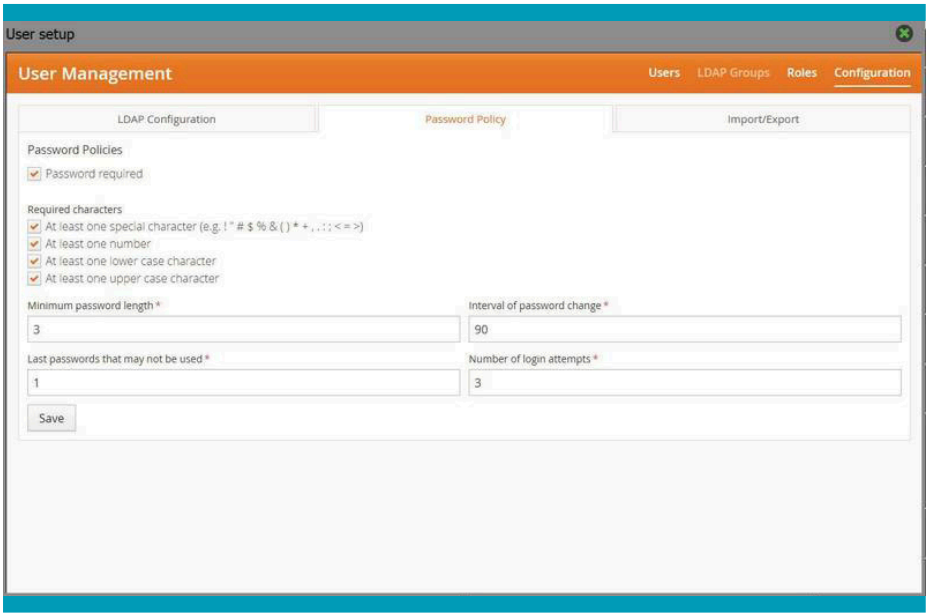
10.3 Configuration de la politique en matière de mots de passe

Pour configurer de la politique en matière de mots de passe, appuyer sur <Configuration> dans le coin en haut à droite et sélectionner l'onglet <Password Policy>. Les éléments suivants peuvent être configurés :

- Caractères requis
- Longueur du mot de passe
- Délai d'expiration du mot de passe (en jours)
- Derniers mots de passe à ne pas utiliser
- Nombre maximum de tentatives de connexion

Remarque: Les modifications apportées à la politique en matière de mots de passe n'affectent que les utilisateurs créés par la suite. Les utilisateurs déjà créés ne seront pas affectés.

Remarque : La politique en matière de mots de passe LDAP pour le compte LDAP l'emporte sur la politique en matière de mots de passe.



Écran 10.18: Configuration de la politique en matière de mots de passe

10.4 Importation et exportation des paramètres de gestion des utilisateurs

La configuration UMS peut être transférée d'un instrument à un autre. Ce processus se fait en deux étapes :

(1) Copie entre la clé USB et le dossier d'échange UMS à l'aide de l'outil UMS Exchange

(2) Importation dans/Exportation vers l'UMS dans la configuration User Management.

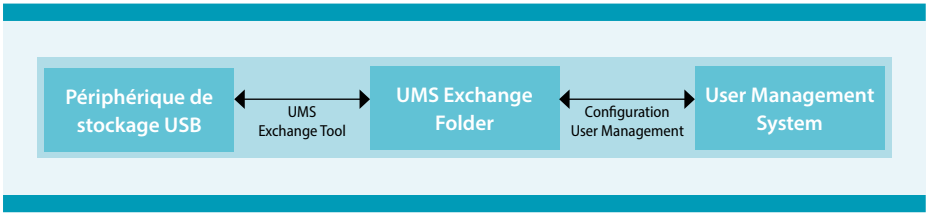


Figure 10.2: User Management System (Système de gestion des utilisateurs)

La procédure donnée en exemple s'applique aux deux types de fichiers suivants :

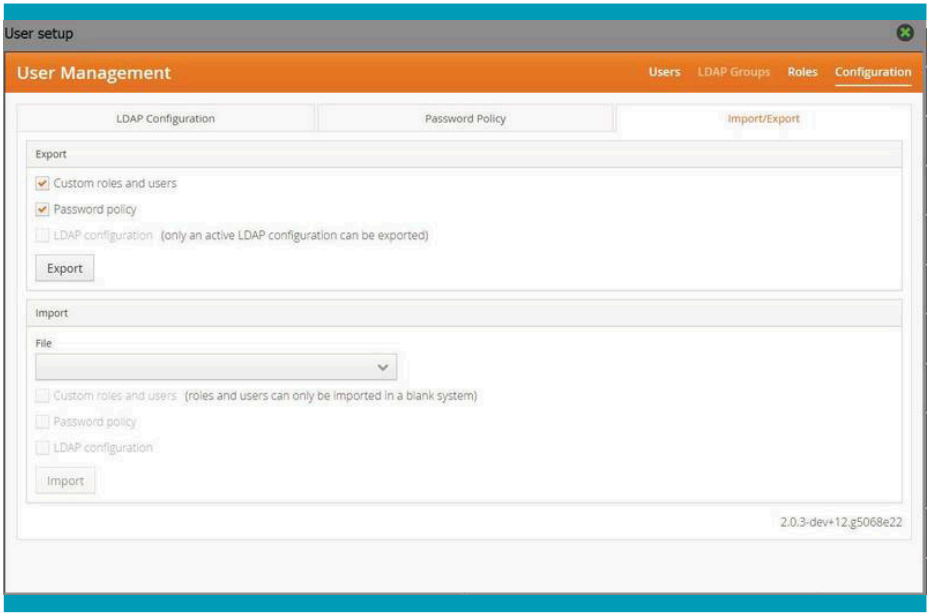
- Importation des fichiers de certificat Secure Sockets Layer (SSL) pour la configuration d'une connexion LDAP sécurisée.
- Importation et exportation des fichiers de paramètres UMS pour sauvegarde ou réutilisation sur d'autres appareils avec UMS.

Remarque: Seuls les utilisateurs UMS ayant le rôle d'administrateur « Administration tools user » ont accès à cette application.

10.4.1 Exportation des paramètres de gestion des utilisateurs

IMPORTANT
Les rôles et les utilisateurs peuvent uniquement être importés dans un système vierge.

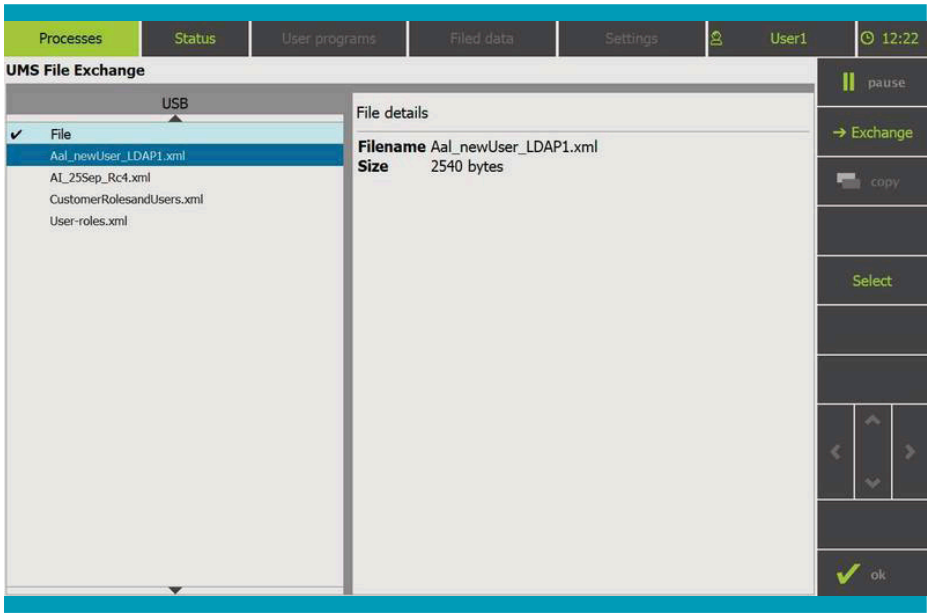
1. Insérer une clé USB.
2. Aller dans <User Management> ▸ <Configuration> ▸ <Import/Export>. Appuyer sur <Export> (Exporter). Les paramètres UMS sont exportés vers le dossier UMS Exchange Folder sur l'instrument.



Écran 10.19: Sous-menu « Configuration » avec onglet « Import/Export » actif

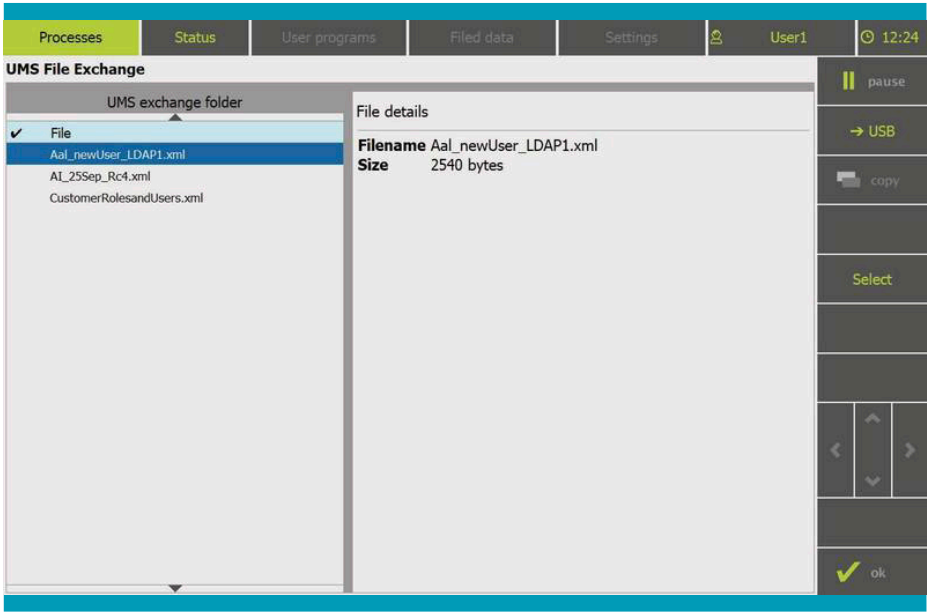
3. Pour accéder à <UMS File Exchange>, aller dans <Settings> ▸ <Tools>, < UMS File Exchange>, et appuyer sur <run>.

4. Si USB est affiché dans la colonne de gauche, appuyer sur <Exchange> pour afficher le contenu du dossier d'échange UMS (voir Écran 10.20). Les fichiers du dossier d'échange UMS s'affichent alors dans la colonne de gauche (voir Écran 10.21).



Écran 10.20: Fichier sélectionné et bouton de menu « Exchange »

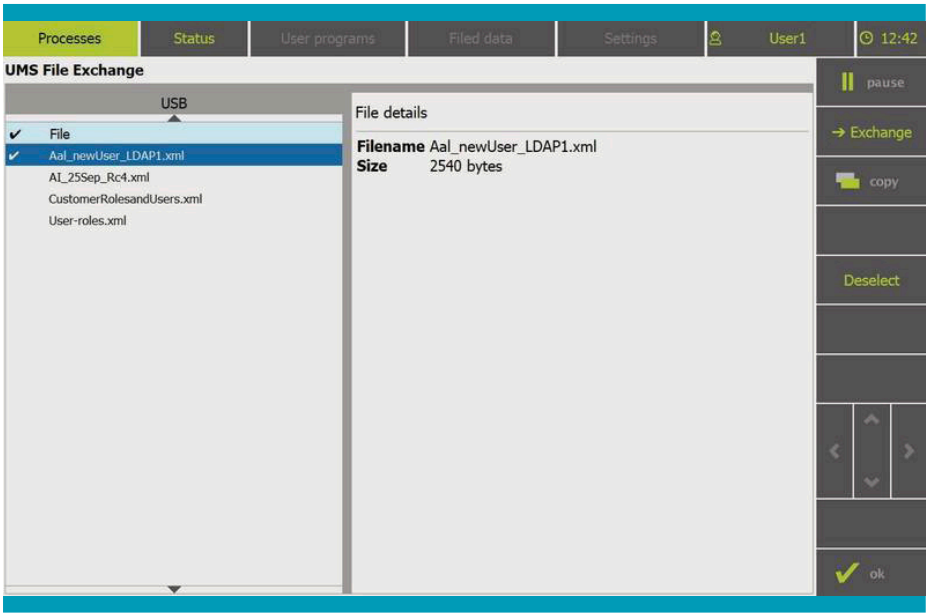
5. Sélectionner les fichiers à transférer vers l'UMS et appuyer sur <Select>.
6. Une fois tous les fichiers à transférer sélectionnés, appuyer sur <copy> pour démarrer le transfert.



Écran 10.21: Dossier d'échange UMS avec les fichiers sélectionnés

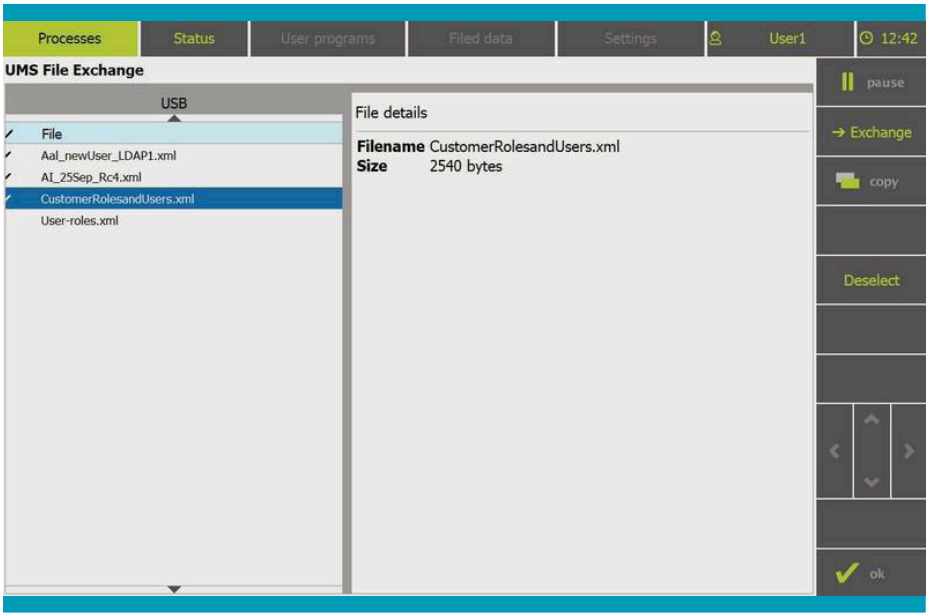
10.4.2 Importation des paramètres UMS

1. Insérer une clé USB.
   Vérifier que tous les fichiers se trouvent dans le dossier racine de la clé USB (les fichiers enregistrés dans les sous-dossiers ne sont pas reconnus).
2. Aller dans **<Process>** ▸ **<Tools>**, **<UMS File Exchange>**, et appuyer sur **<run>** pour accéder à l'outil **<UMS File Exchange>**. Une liste de fichiers s'affiche à gauche.
3. Lorsque le dossier d'échange UMS est affiché, appuyer sur **<USB>** dans la barre d'outils. Vérifier que **<USB>** est affiché en haut de la liste des fichiers dans la colonne de gauche.
4. Sélectionner les fichiers à transférer et appuyer sur **<Select>**. Pour désélectionner un fichier, choisir ce fichier et appuyer sur **<Deselect>**.



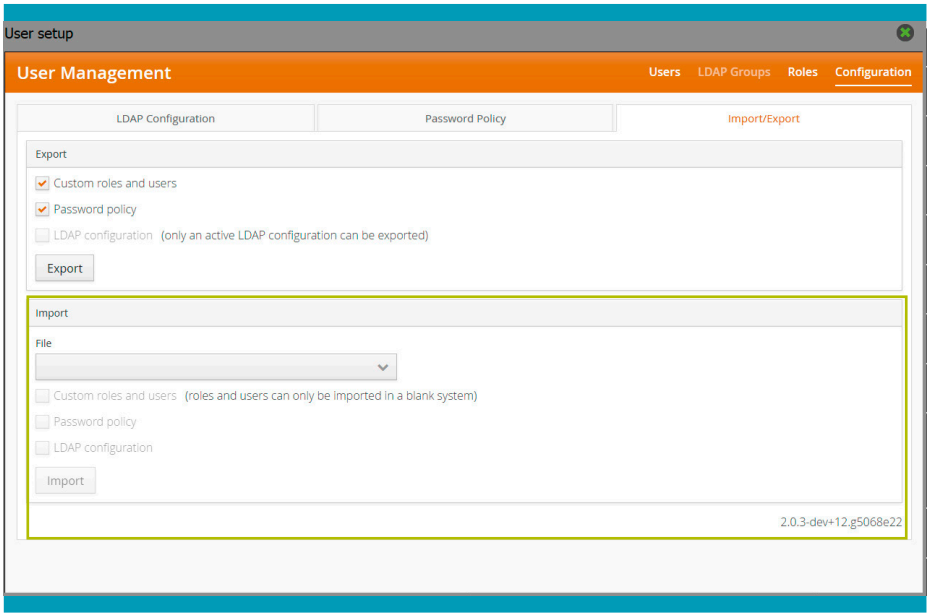
Écran 10.22: Fichier sélectionné et bouton de menu « Select »

5. Une fois tous les fichiers à transférer sélectionnés, appuyer sur <Copy> pour démarrer le transfert.



Écran 10.23: Dossier USB avec les fichiers sélectionnés

6. Aller dans <User setup> ▸ <Configuration> ▸ <Import/Export>. Sélectionner le fichier dans <Import> et appuyer sur <Import>.



Écran 10.24: Sous-menu « Configuration » avec onglet « Import/Export » actif

11 Dépannage

En cas de dysfonctionnement de l'instrument ou d'échec d'un processus, contacter le service Miltenyi Biotec Technical Support au :

+49 2204 8306-3803
technicalsupport@miltenyi.com

Se rendre sur www.miltenyibiotec.com pour obtenir les coordonnés de votre service Miltenyi Biotec Technical Support local.

12
Mentions légales

12.1 Limites de garantie

À l'exception des dispositions figurant dans une déclaration de garantie spécifique qui peut accompagner ce produit de Miltenyi Biotec, ou sauf accord contraire par écrit d'un représentant dûment autorisé de Miltenyi Biotec, la garantie de Miltenyi Biotec couvrant les produits achetés directement auprès de Miltenyi Biotec sera régie par les conditions générales de vente selon lesquelles les produits vous ont été fournis par le revendeur Miltenyi Biotec correspondant. Ces conditions générales sont disponibles sur demande ou sur www.miltenyibiotec.com. Les conditions générales de vente applicables peuvent varier d'un pays ou d'une région à l'autre. Rien de ce qui est indiqué dans les présentes ne saurait être interprété comme constituant une garantie supplémentaire.

Pour les produits achetés auprès de détaillants ou revendeurs tiers (par ex. achetés auprès d'un distributeur local autorisé par Miltenyi Biotec), des conditions générales différentes peuvent s'appliquer.

Pour connaître la garantie couvrant votre produit, consulter le bordereau de marchandises, la facture, le reçu ou toute autre document commercial. Certains éléments d'une combinaison de produits achetée peuvent avoir une durée de garantie plus courte que celle mentionnée sur le bordereau de marchandises, la facture, le reçu ou toute autre document commerciale (p. ex. biens ayant une durée de vie limitée et sujets à obsolescence).

La garantie de Miltenyi Biotec pour ce produit couvre uniquement les anomalies du produit causées par des défauts de matériau ou de fabrication dans le cadre d'une utilisation normale. Elle ne couvre pas les anomalies du produit causées par une autre raison, y compris, sans s'y limiter, les anomalies du produit dues à une utilisation du produit autre que celle spécifiquement décrite dans ce manuel d'utilisation, par exemple : utilisation inappropriée ou incorrecte ; montage ou installation incorrect par un opérateur ou un tiers ; usure raisonnable ; utilisation, manipulation, stockage, maintenance ou entretien négligent ou incorrect ; non-

respect des instructions de fonctionnement ; modification non autorisée d'un composant de ce produit ; utilisation de consommables, accessoires ou matériaux inappropriés.

La garantie de Miltenyi Biotec ne couvre pas les produits vendus TELS QUELS ou AVEC TOUS LES DÉFAUTS, ni les consommables. Rien de ce qui est indiqué dans les présentes ne saurait être interprété comme constituant une garantie supplémentaire.

Miltenyi Biotec doit impérativement être informé sans délai en cas de réclamation formulée dans le cadre de cette garantie. Si un défaut de matériau ou de fabrication apparaît pendant la période de garantie, Miltenyi Biotec prendra les mesures nécessaires pour rétablir la complète utilisabilité de l'instrument.

Limitation des dommages
Miltenyi Biotec ne saurait être tenu pour responsable des dommages indirects ou consécutifs résultant du non-respect d'une garantie ou disposition implicite ou explicite à l'égard de ce produit.

Certains pays/états ou certaines juridictions n'autorisant pas l'exclusion ou la limitation des dommages indirects ou consécutifs, les limitations ou exclusions ci-dessus peuvent ne pas s'appliquer dans votre cas. Cette déclaration de garantie vous confère des droits légaux spécifiques, mais vous pouvez également avoir d'autres droits, qui varient d'un état ou d'une juridiction à l'autre.

12.2 Marques commerciales

CliniMACS, CentriCult et le logo Miltenyi Biotec sont des marques ou marques déposées de Miltenyi Biotec et/ou de ses filiales dans différents pays du monde.

ANNEXE

Chaque processus, outil et paramètre est associé à des droits spécifiques, p. ex. le droit « Show » (Afficher) et le droit « Start » (Démarrer). Avec le droit « Show », l'outil/le processus/le paramètre sera visible dans l'onglet Process/Settings (Processus/Paramètres). Pour pouvoir exécuter le processus/l'outil/le paramètre, le droit « Start » doit être attribué au rôle. Les composants plus complexes, comme la piste d'audit et la gestion des utilisateurs, disposent de droits plus détaillés.

Processus/Outil/Paramètres/ Composant	Détails
Process xxx right (Droit pour le processus xxx)	• Show process xxx (Afficher le processus xxx) • Start process xxx (Démarrer le processus xxx)
Tool xxx right (Droit pour l'outil xxx) • Backup Filed Data (Sauvegarde des données archivées) • Custom Files (Fichiers personnalisés) • Instrument check (Contrôle de l'instrument) • License (Licence) • N2 Settings (Paramètres N2) • Network Settings (Paramètres réseau) • Set Time (Régler l'heure) • Settings Exchange (Partage de paramètres) • SetVolume (RéglerVolume) • Shutdown (Arrêt) • UMSFileExchange exchange (Partage PartageFichierUMS) • UMSSettings settings Process xxx right (Paramètres UMS Droit pour le processus xxx)	• Show tool xxx (Afficher l'outil xxx) • Start tool xxx (Démarrer l'outil xxx)

Processus/Outil/Paramètres/ Composant	Détails
Setting xxx right (Droit pour le paramètre xxx) • Info (Info) • System settings (Paramètres du système)	• Show setting xxx (Afficher le paramètre xxx) • Start setting xxx (Démarrer le paramètre xxx)
Instrument (Instrument)	• Log file access via FTP (Accès au fichier journal via FTP) • Show injected programs (Afficher les programmes injectés) • Start injected programs (Démarrer les programmes injectés)
User Management (Gestion des Utilisateurs)	• Assign role (Attribuer un rôle) • Configure LDAP connection (Configurer la connexion LDAP) • Create role (Créer un rôle) • Create user (Créer un utilisateur) • Export (Exporter) • Import (Importer) • Read Password Policy (Lire la politique en matière de mots de passe) • Read details of foreign account (Lire les détails d'un autre compte) • Read details of own account (Lire les détails de son propre compte) • Read own user details (Lire les détails de son propre profil utilisateur) • Read rights of foreign account (Lire les droits d'un autre compte) • Read rights of own account (Lire les droits de son propre compte) • Read role (Lire le rôle) • Read user details (Lire les détails du profil utilisateur) • Set user active (Définir l'utilisateur comme actif) • Set user inactive (Définir l'utilisateur comme inactif) • Unlock user (Déverrouiller l'utilisateur) • Update Password Policy (Mettre à jour la politique en matière de mots de passe) • Update own user details (Mettre à jour les détails de son propre profil utilisateur) • Update role (Mettre à jour le rôle) • Update user details (Mettre à jour les détails du profil utilisateur)
Audit Trail Management (Gestion de la piste d'audit)	• Export audit trail events (Exporter les événements de la piste d'audit) • Read audit trail events (Lire les événements de la piste d'audit) • Reset audit trail events (Réinitialiser les événements de la piste d'audit)

Processus/Outil/Paramètres/ Composant	Détails

Tableau A.1: Aperçu des droits définis dans le logiciel

Rôles par défaut

Rôles	Outils/droits
ATS User (Utilisateur ATS)	Utilisateur du système Audit Trail • Audit Trail Management (Gestion de la piste d'audit)
Administration tools user (Utilisateur des outils d'administration)	• Customer settings (Paramètre client) • Network settings (Paramètres réseau) • Platform configuration settings (Paramètres de configuration de la plateforme) • Settings exchange (Partage de paramètres) • System settings (Paramètres du système) • UMSFileExchange exchange (Partage PartageFichierUMS)
File management user (Utilisateur des outils de gestion des fichiers)	Utilisateur des outils de gestion des fichiers • Backup Filed Data (Sauvegarde des données archivées) • Custom Files (Fichiers personnalisés) • Log file access via FTP (Accès au fichier journal via FTP)
File system access (Accès au système de fichiers)	Accès aux fichiers exécutables arbitraires dans le système de fichiers – pas d'accès aux droits
Support tools user (Utilisateur des outils de support)	Utilisateur des outils prenant en charge l'exécution des applications • Chamber In (Entrée de chambre) • Chamber out (Sortie de chambre) • FormU Sensor (Capteur FormU) • FormU Valves (Valves FormU) • FRAMrd • Gasmix Settings (Paramètres du mélange gazeux) • Instrument check (Contrôle de l'instrument) • Module Settings (Paramètres du module) • Sealer (Soudeuse)
UM Administrator (Administrateur GU)	Administrateur du composant de gestion des utilisateurs « User Management » – tous les droits
UM Service (Service GU)	Service User (Utilisateur service) • User Management – all rights (Gestion des utilisateurs – tous les droits)
UM User (Utilisateur GU)	Customer user (Utilisateur client) • User Management: Read details for own account (Gestion des utilisateurs : lire les détails de son propre compte) • User Management: Read rights for own account (Gestion des utilisateurs : lire les droits de son propre compte)

Tableau A.2: Rôles par défaut

Miltenyi Biotec

Allemagne/Autriche
Miltenyi Biotec B.V. & Co. KG
Friedrich-Ebert-Straße 68
51429 Bergisch Gladbach
Allemagne
+49 2204 8306-0
+49 2204 85197
macsde@miltenyi.com

États-Unis/Canada
Miltenyi Biotec, Inc.
1201 Clopper Road
Gaithersburg, MD 20878
États-Unis
800 FOR MACS
+1 866 811 4466
+1 877 591 1060
macsus@miltenyi.com

Australie
Miltenyi Biotec Australia Pty. Ltd.
Unit 11, 2 Eden Park Drive
Macquarie Park NSW 2113
Australie
+61 2 8877 7400
+61 2 9889 5044
macsau@miltenyi.com

Benelux
Miltenyi Biotec B.V.
Dellaertweg 9C
2316 WZ Leiden
Pays-Bas
macsnl@miltenyi.com
Service clientèle pour:
les Pays-Bas
0800 4020120
0800 4020100
Belgique
0800 94016
0800 99626
Luxembourg
800 24971
800 24984

Chine
Miltenyi Biotec Technology & Trading (Shanghai) Co., Ltd.
Room A401, 4/F
No. 1077, Zhangheng Road
Pudong New Area
201203 Shanghai
P.R. Chine
+86 21 6084 0210
+86 21 6235 0953
macscn@miltenyi.com.cn

Corée du Sud
Miltenyi Biotec Korea Co., Ltd.
Donggeuk 7F
562 Nonhyeon-ro
Gangnam-gu
Seoul 06136
Corée du Sud
+82 2 555 1988
+82 2 555 8890
macskr@miltenyi.com

Espagne
Miltenyi Biotec S.L.
C/Virgilio 2, Edificio II, Planta –1
28223 Pozuelo de Alarcón, Madrid
Espagne
+34 91 512 12 90
+34 91 512 12 91
macses@miltenyi.com

États nordiques et baltes
Miltenyi Biotec Norden AB
Medicon Village
Scheeletorget 1
223 81 Lund
Suède
macsse@miltenyi.com
Service clientèle pour:
Suède
0200 111 800
+46 280 72 99
Danemark
80 20 30 10
+46 46 280 72 99

Norvège, Finlande, Islande et pays baltes
+46 46 280 72 80
+46 46 280 72 99

France
Miltenyi Biotec SAS
10 rue Mercoeur
75011 Paris
France
+33 1 56 98 16 16
macsfr@miltenyi.com

Hongkong
Miltenyi Biotec Hong Kong Ltd.
Unit 301, Lakeside 1
No. 8 Science Park West Avenue
Hong Kong Science Park
Pak Shek Kok, New Territories
Hongkong
+852 3751 6698
+852 3619 5772
macshk@miltenyi.com.hk

Inde
Miltenyi Biotec India Pvt. Ltd.
Ground Floor, Lab No. E 101/1,
Building no. 3600
Plot No. 4, Sy. no. 101,
Neovantage Park,
Synergy Square 3 Genome Valley,
Lalgadimalakpet
Medchal Malkajgiri, Shamirpet (M)
Telangana 500101
Inde
+91 040 45175910
macsin@miltenyi.com

Italie
Miltenyi Biotec S.r.l.
Via Paolo Nanni Costa, 30
40133 Bologna
Italie
+39 051 6 460 411
+39 051 6 460 499
macsit@miltenyi.com

Japon
Miltenyi Biotec K.K.
NEX-Eitai Building 5F
16-10 Fuyuki, Koto-ku
Tokyo 135-0041
Japon
+81 3 5646 8910
+81 3 5646 8911
macsjp@miltenyi.com

Royaume-Uni
Miltenyi Biotec Ltd.
Almac House, Church Lane
Bisley, Surrey GU24 9DR
Royaume-Uni
+44 1483 799 800
+44 1483 799 811
macsuk@miltenyi.com

Singapour
Miltenyi Biotec Asia Pacific Pte Ltd.
438B Alexandra Road, Block B
Alexandra Technopark
#06-01
Singapour 119968
+65 6238 8183
+65 6238 0302
macssg@miltenyi.com

Suisse
Miltenyi Biotec Swiss AG
Soodstrasse 52
8134 Adliswil
Suisse
+41 32 623 08 47
+49 2204 85197
macsch@miltenyi.com

www.miltenyibiotec.com

Miltenyi Biotec fournit des produits et des services dans le monde entier. Rendez-vous sur **www.miltenyibiotec.com/local** pour trouver votre interlocuteur Miltenyi Biotec le plus proche.

CliniMACS, CentriCult et le logo Miltenyi Biotec sont des marques ou marques déposées de Miltenyi Biotec B.V. & Co. KG et/ou de ses filiales dans différents pays du monde. Copyright © 2026 Miltenyi Biotec et/ou ses filiales. Tous droits réservés.

210-005-266/01 | Édition : 2026-03